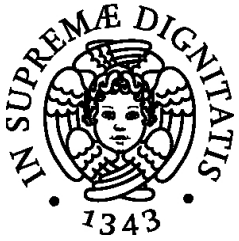


Università di Pisa

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea Magistrale in Matematica

Tesi di Laurea Magistrale

A survey on Diophantine results

Candidato:
Roberto Pirisi

Relatore:
Prof. Roberto Dvornicich

Controrelatore:
Prof. Ilaria Del corso

Anno Accademico 2011/2012

Introduction

Diophantine problems have historically been one of the first motivations for the development of mathematics. While troughout the centuries mathematical knowledge deeply evolved, diophantine problems have always been a motivation for further study, and to present day they are a pushing force for many branches of mathematics.
In this dissertation we'll introduce the reader to some typical kind of questions, and answers, one can find in the study of such matters. The modern point of view on the study of diophantine equations has been basically redefined in the twentieth century, with the reshaping of algebraic geometry by Alexander Grothendieck, Jean-Pierre Serre and many others. The instruments of algebraic geometry have brought solutions to many unsolved problems, the most famous being Fermat's Last Theorem.

The first chapter will be dedicated to developing the needed algebraic and geometric tools, starting by the classical tools of Algebraic Number Theory, such as discrete valuation rings, Dedekind domains, number fields, absolute values, completions, product formulas and heights. These instruments, while largely classical, are still fundamental to the study of diophantine problems. In the second part of the first chapter, we'll develop the instruments of algebraic geometry we'll need in the rest of the dissertation. We'll suppose the reader has a basic knowlege of scheme theory, and develop the theory of normal schemes, sheaves of $\mathcal{O}_X$-modules, invertible sheaves, Picard group, divisor classes, degree of a finite morphism, pullback and pushforward of sheaves and divisors, curves and morphism of curves, leading to what is possibly the most important result of curve theory, the Riemann-Roch theorem. Cohomology theory and the thoery of kähler differentials will just be hinted.

In the second chapter, we'll prove a classical result by Siegel: an affine algebraic curve having infinitely many points with integral coefficients must have genus zero and at most two points at infinity. First we'll state this result in a more modern way, defining the concept of Quasi-S integral points, which translates the concept of points whose coefficients has denominator divisible only by a fixed finite set of primes to the setting of abstract algebraic varieties. We'll show how to simplify the problem of proving Siegel's theorem by reducing step by step to a single basic case, that of a curve with genus zero and three points at infinity.
In the second section of the chapter, given an absolute value v over a number field k, we'll extend the v-adic topology defined on k to any abstract algebraic variety over k, and prove it behaves well with respect to morphisms. Finally, we'll show the v-adic topology has good compactness properties when k is complete and locally compact with respect to the v-adic topology. In the last part of the second chapter, we'll prove Siegel's theorem. This

will be a combined application of the Riemann-Roch theorem, the v-adic topology, and finally Schmidt's Subspace Theorem, in the form proposed by Schlickewei, a powerful theorem on approximation of algebraic numbers, a subject deeply tied to diophantine problems, which will allow us to conclude.

The third chapter will be dedicated to Hilbert's Irreducibility Theorem, another classical result stating that given a number field k and a finite set of irreducible polynomials $f_1, \dots, f_r \in k[x_1, \dots, x_n, y_1, \dots, y_m]$ and $g \in [y_1, \dots, y_m]$, there are always infinite m-uples $(\alpha_1, \dots, \alpha_m)$ with coefficients in k such that $f_i(x_1, \dots, x_r, \alpha_1, \dots, \alpha_m)$ remains irreducible for all $i \in \{1, \dots r\}$, and $(\alpha_1, \dots, \alpha_m)$ is not a zero of g. While the statement of Hilbert's Irreducibility Theorem is purely arithmetical, it is deeply tied to algebraic geometry.
In the first section, we'll prove the Irreducibility Theorem. Our main instruments will be basic Galois Theory, Siegel's Theorem and the Riemann Roch Theorem. We'll proceed by showing that the proof boils down to the case of two variables, then we'll use Siegel's Theorem and Riemann-Roch to reduce to an easily provable diophantine property, the fact that the image of integral points trought a morphism of degree greater than one has asymptotic density zero. We'll then answer some very natural questions about such density problems.
In the last section, we'll introduce the problem of Universal Hilbert sets. Hilbert Universal sets are subsets of the integers of a field k with the following property:

For all irreducible polynomials $f \in k[X, Y]$, there are only finite $\alpha \in H$ such that $f(X, \alpha)$ is reducible.

We'll show that given a number field k, there is always a Universal Hilbert set with respect to k, we'll answer some questions about the density of such sets, and we'll explicitly show a three-parameters family of Universal Hilbert sets.

Contents

Chapter 1

Some prerequisites

In this chapter we're going to develop a few algebraic, number theorethic and geometric prerequisites needed for the rest of this dissetation; the expert reader may be able to skip the more basic parts of the chapter.

1.1 DVR and Dedekind domains

First, we'll show some properties of two very simple kind of integral domains: Discrete Valuation Rings, which we'll call simply DVR form now on, and Dedekind domains. These two kind or rings are very simple, yet they are fundamental in both Algebraic Number Theory and Algebraic Geometry.

Definition 1.1.1. Let K be a field. A *Discrete Valuation* over K is a function $\mathrm{v} : K \to \mathbb{Z} \cup \{\infty\}$ satisfying the following conditions:

1. $\mathrm{v}(ab) = \mathrm{v}(a) + \mathrm{v}(b)$.
2. $\mathrm{v}(a+b) \geq \min(\mathrm{v}(a), \mathrm{v}(b))$.
3. $\mathrm{v}(a) = \infty \Leftrightarrow a = 0$.
4. v does not assume only 0 and ∞ as values.

We call an integral domain R *Discrete Valuation Ring* if its field of fractions is equipped with a discrete valuation such that $R = \mathrm{v}^{-1}(\mathbb{N} \cup \infty)$.

Remark 1.1.1.

- *if a is a root of unit,* $\mathrm{v}(a) = 0$
- *If K is endowed with a discrete valuation* v, $R \doteq \mathrm{v}^{-1}(\mathbb{N} \cup \infty)$ *is a DVR.*
- *If $a \in R^* \Leftrightarrow \mathrm{v}(a) = 0$.*
- *If $a \in K$, then either $a \in R$ or $a^{-1} \in R$.*

Proof.

- This is clear as $\mathrm{v}(a^n) = n\mathrm{v}(a)$.
- We just need to show R is a ring: condition (1) of the definition implies R is multiplicatively closed, condtion (2) implies R is additively closed, condition (3) implies $0 \in R$, and we just proved that $1 \in R$.
- Suppose $a \in R^*$: as $aa^{-1} = 1$, the valuation of $a^{-1} \in R$ is negative unless it is zero. Conversely, if $\mathrm{v}(a) = 0$ then $\mathrm{v}(a^{-1}) = 0$ and $a \in R^*$.
- This is clear as $\mathrm{v}(a^{-1}) = -\mathrm{v}(a)$.

□

As we're going to see, DVR are exceedingly simple rings:

Proposition 1.1.2. *Let R be a Noetherian integral domain. The following conditions are equivalent:*

1. *R is a DVR.*
2. *There is an element π of R (which we call* parameter*) such that all nontrivial ideals of R are generated by a power of π.*
3. *There is an ideal m of R such that all nontrivial ideals of R are powers of m*
4. *R is a local regular ring of dimension* 1*.*
5. *R is local, integrally closed of dimension* 1

Proof.

$1 \Rightarrow 2$ Choose $a \in R$ such that the valuation of a is minimal. If there was $b \in R$ such that $\mathrm{v}(a)$ did not divide $\mathrm{v}(b)$, we could find c with $\mathrm{v}(c) = \mathrm{GCD}(\mathrm{v}(a), \mathrm{v}(b)) < \mathrm{v}(a)$, which is not possible. then, if $\mathrm{v}(b) = m\mathrm{v}(a)$, $b = a^m\alpha$, with $\alpha \in R^*$, and we can choose a as our parameter.

$2 \Leftrightarrow 3$ $2 \Rightarrow 3$ is trivial. Suppose now (3) holds. Let then $a \in m \setminus m^2$. As the ideal $\langle a \rangle$ is a power of m not contained in m^2, $m = \langle a \rangle$.

$2 \Leftrightarrow 4$ $2 \Rightarrow 4$ is trivial. To show $4 \Rightarrow 2$, let $\langle \pi \rangle$ be the maximal ideal of R, which is principal as R is regular. By the *Nakayama's Lemma*, $\cap_{n\in\mathbb{N}}\{\pi\}^n = 0$, so given $a \in R$ there is $m_a \in \mathbb{N}$ such that $a = \pi^{m_a}\alpha$, with α a unit of R. Then, given an ideal I, let m_I be the minimum of these integers taken on the elements of I. Clearly $I = \langle \pi^{m_I} \rangle = \langle \pi \rangle^{m_I}$.

$4 \Leftrightarrow 5$ The implication $4 \Rightarrow 5$ is a consequence of the fact that R is factorial (by (2), which we have shown to be implied by (4)) which implies it is integrally closed. To show $5 \Rightarrow 4$ we only need to show that

the maximal ideal M of R is principal. Let a be a nonzero, nonunit element of R; as R is noetherian and local of dimension one, there is n such that $M^n \subseteq \langle a \rangle$ (just consider the primary decomposition of $\langle a \rangle$). Let n' be the maximum integer ≥ 0 such that $M^{n'}$ is not contained of $\langle a \rangle$. If $n' = 0$, $M = \langle a \rangle$ and our thesis is satisfied. If $n' > 0$, choose $b \in M^{n'}, b \notin \langle a \rangle$, and let x be $\frac{b}{a}$ in the field of fractions of R. As $b \notin \langle a \rangle$, $x \notin R$. Now, by construction $xM \subset R$ is an ideal of R; if xM were to be a proper ideal of R, it would be a faithful $R[x]$-module, finite as an R-module, which would imply x is integral over R. This is not possible as $x \notin R$ and R is integrally closed.

$2 \Rightarrow 1$ Given $\frac{a}{b}$ in the field of fractions of R, put $\mathrm{v}(\frac{a}{b}) = m_a - m_b$, where m_a and m_b are the constants we defined above. It's easy to see this is a discrete valuation making R into a DVR.

□

As intuition suggests, a DVR can only describe the objects we're intrested in "locally". A more general object to study are Dedekind domains, which, as we'll see, are rings which look locally as DVRs.

Definition 1.1.2. A *Dedekind domain* is a noetherian, integrally closed domain of dimension 1.

Proposition 1.1.3. *Let D be a noetherian integral domain. The following properties are equivalent:*

1. *D is a Dedekind domain.*
2. *For all nonzero primes P of D the localization D_P is a DVR.*
3. *D has dimension 1 and all the primary ideals of D are powers of a prime ideal.*

Proof.

$1 \Leftrightarrow 2$ This is implied by the previous proposition as integral closure is a local property, dimension doesn't change when localizing by a nonzero prime ideal, and the dimension of a ring is the supremum of the dimensions of its localizations.

$2 \Leftrightarrow 3$ The bijective correspondence beetween primary ideals of a localization D_P and primary ideals of R contained in P immediately implies every primary ideal of R is the power of a prime ideal. Now, suppose (3) holds, and consider the localization D_P by a nonzero prime ideal P. Let $a \in P \setminus P^2$; as the radical of $\langle a \rangle$ is P, again by the bijective correspondence $\langle a \rangle = P^n$ for some n, and thus $\langle a \rangle = P$.

□

A special example of a Dedekind domain is $\mathbb{Z}$. As we're about to see, a Dedekind domain acts similarly to a unique factorization domain, but a factorial Dedekind domain is necessarily a much simpler ring, a principal ideal domain, as is the case with $\mathbb{Z}$.

Proposition 1.1.4. *Let D be a dedekind domain, I an ideal of D. Then there is a factorization $I = P_1 \dots P_r$, unique up to the order of factors, where $P_1, \dots, P_r$ are prime ideals. Also, a Dedekind domain is UFD if and only if it is PID.*

Proof. Let I be a nonzero ideal of D; as D is noetherian, I has a primary factorization $I = Q_1 \dots Q_s$. It is now sufficient to notice that $Q_1, \dots Q_r$ are powers of prime ideals $M_1, \dots, M_t$ (which are unique due to the unicity of the radicals in the primary factorization) and the exponents are clearly unique, or else for some index i we would have ${M_i}^k = {M_i}^{k+q}$ in the localization and thus $M_i = 0$.
For the second part of the proposition, it suffices to notice that an UFD of dimension 1 is a PID; let P be a nonzero prime ideal of D, then there must be an irreducible element $a \in P$. Then, as $\langle a \rangle$ is a prime ideal, we must have $\langle a \rangle = P$. □

Now, given a prime ideal P of a dedekind domain, as D_P is a DVR, it induces a valuation (the P-adic valuation v_P) on the field of fractions of D, which we'll call K.

Proposition 1.1.5. *A Dedekind domain is the intersection of its localizations. In particular, if $x \in K$, then $x \in D$ if and only if $v_P(x) \geq 0$ for all P.*

Proof. First, notice that if the valuation of $b \in D$ is zero for all prime ideals of D, $b \in D^*$. Now, consider $\frac{a}{b} \in K$, with $\langle a \rangle \nsubseteq \langle b \rangle$, and suppose all its valuations are ≥ 0, which is the same as saying $\frac{a}{b}$ belongs to the intersection of all the localizations of D: then for all P we have $\mathrm{v}_P(a) \geq \mathrm{v}_P(b)$; as clearly $v_P(I)$ is the exponent of P in the prime ideal factorization of I, this implies $\langle a \rangle \subseteq \langle b \rangle$. □

We are now going to develop an instrument to measure the amount to which a dedekind domain fails to be an UFD: the *Ideal class group*. This is a fundamental instrument of algebraic number theory.

Definition 1.1.3. Let D be an integral domain, K its field of fractions. A *fractional ideal* of D is a D-submodule M of K such that there is $a \in D$ with $aM \subseteq D$. In particular, any ideal of D is a fractional ideal. a fractional ideal M is said to be invertible if there is a fractional ideal N such that $MN = D$.

Clearly a nonzero principal fractional ideal (u) is invertible, with inverse (u^{-1}); as we'll see, the peculiarity of a Dedekind domain is that its fractional ideals form a group with respect to ideal multiplication.

Proposition 1.1.6. *An invertible ideal is finitely generated as a D-module.*

Proof. First, if $MN = D$ then N is unique and is equal to $(D : M)$. Now, there are $x_1, \ldots, x_n \in M$, $y_1, \ldots, y_n \in N$ such that $\sum_{i=1,\ldots,n} y_i x_i = 1 \in D$. Then, if $x \in M$, $x = x \sum_{i=1,\ldots,n} y_i x_i = \sum_{i=1,\ldots,n} (xy_i)x_i$. As xy_i belongs to D for all i, M is generated by $x_1, \ldots, x_n$. □

Proposition 1.1.7. *Let M be a finitely generated fractional ideal. The following are equivalent:*

1. *M is invertible.*
2. *M_P is invertible as a fractional ideal of D_P for all prime ideals P.*
3. *M_m is invertible as a fractional ideal of D_m for all maximal ideals m.*

Proof.

$1 \Rightarrow 2$ $A_p = (M(D : M))_P$, and as M is finitely generated $(M(D : M))_P = M_P(D : M)_P = M_P(D_P : M_P)$, therefore M_P is invertible.

$2 \Rightarrow 3$ obvious.

$3 \Rightarrow 1$ Let $I = M(D : M)$ which is an ideal of D. As M is finitely generated $I_m = M_m(D_m : M_m) = D_m$; then I cannot be a subset of any maximal ideal of D, and thus $I = D$.

□

Lemma 1.1.8. *Let R be a local integral domain. R is a DVR if and only if every nonzero fractional ideal of R is invertible.*

Proof. One implication is easy: if R is a DVR m its maximal ideal and let I be a fractional ideal of R. Then there is $x \in R$ such that Ix is an ideal of R, which means $Ix = m^n$, with n possibly zero. Then the fractional ideal $Rx\pi^{-n}$ is its inverse.
To prove the other implication, first notice that all ideals of R are invertible and thus finitely generated, implying R is noetherian. Let now Σ be the set of ideals of R not equal to any power of the maximal ideal m. Consider now an ascending chain $I_j \in \Sigma$; as R is noetherian, if $\cup_j I_j = m^n$ there would be an index j such that all of m^n's generators belong to I_j, which is not possible. We can then apply Zorn's lemma and obtain a maximal element $\mathcal{I}$ of Σ. As $\mathcal{I} \neq m$, $m \supset \mathcal{I}$ and $m^{-1}\mathcal{I}$ is a proper ideal of R. If $m^{-1}\mathcal{I} = \mathcal{I}$, then we would have $\mathcal{I}m = \mathcal{I}$ and by Nakayama's lemma $\mathcal{I}$ would be the zero ideal, and our thesis would be satisfied. If $m^{-1}\mathcal{I} \supset \mathcal{I}$ then $m^{-1}\mathcal{I} = m^n$ for some n, which would imply $\mathcal{I} = m^{n+1}$, contradicting our hypotesis. □

Proposition 1.1.9. *Let D be an integral domain. D is a Dedekind domain if and only if every nonzero fractional ideal is invertible.*

Proof. Suppose D is a Dedekind domain. As D is noetherian, any fractional ideal I is finitely generated, and as for any nonzero prime ideal P of D the localization is a DVR, the third condition of Proposition (1.1.7) is met and I is invertible.
To show the converse is true, first we notice that as all ideals of D are invertible, thus finitely generated, D is noetherian. We just need to show its localizations at nonzero prime ideals are DVR. To do this it suffices to show that given any nonzero prime ideal P the ideals of D_P are all invertible, then by the last lemma D_P will be a DVR. Let I be a nonzero ideal of D_P, then its contraction $I^c = I \cap D$ is a nonzero ideal of D, and there is J such that $I^C J = D$, thus $IJ_P = D_P$. □

Then, given a Dedekind domain, the set of its nonzero fractional ideals forms an abelian group, the ideal group od D. This group, however, is too big to yield much useful information on D. To simplify it, first we notice that the principal fractional ideals are a subgroup of D, thus a normal subgroup as the ideal group is abelian. Then D is a UFD if and only if the subroup of principal fractional ideals is the whole ideal group, which suggests the correct object we should study:

Definition 1.1.4. Let $I(D)$ be the class group of a Dedekind domain D, and $P(D)$ the subgroup of principal fractional ideals. The *Ideal class group* of a Dedekind domain D is the quotient $I(D)/P(D)$, and we write it $\mathrm{Cl}(D)$.

For those who are familiar with algebraic geometry, there is no confusion in naming the ideal class group $\mathrm{Cl}(D)$, as it is exactly the class group of $\mathrm{spec}(D)$.

The two main Types of Dedekind domain we're intrested in are the ring of sections of a curve over a field k and the ring of integers of a finte extension of $\mathbb{Q}$; in this section we'll concentrate on the latter. First, we must prove the ring of integers of a number field is a Dedekind domain:

Definition 1.1.5. Let k be a number field. The *ring of integers* of k, which we name $\mathcal{O}_k$, is the integral closure of $\mathbb{Z}$ in k.

Lemma 1.1.10. *Let D be an integrally closed domain, K its field of fractions, and L a finite separable extension of K. Then there is a basis $\{\gamma_1, \ldots, \gamma_r\}$ of L over K such that the integral closure of D in L is a sub D-module of $\gamma_1 D \oplus \ldots \oplus \gamma_r D$.*

Proof. First, given an element $l \in L$ it satisfies a polynomial equation over K in the form $a_0 l^n + \ldots + a_n = 0$ where the coefficients a_i are elements of

D. Multiplying this equation by ${a_0}^{n-1}$ we see that $a_0 l$ is integral over D. Therefore, given any basis of L over K we can obtain a basis $\alpha_1, \ldots, \alpha_r$ such that the α_i are integral over D.
Now, as L/K is separable, the bilinear form $(x, y) \to \mathrm{Tr}(xy)$ is nondegenerate and we can choose a dual basis $\gamma_1, \ldots, \gamma_r$ such that $\mathrm{Tr}(\alpha_i \gamma_j) = \delta_{ij}$. Let now x be integral over D, $x = \gamma_1 x_1 + \ldots + \gamma_r x_r$, with x_j in K for all j. $x\alpha_i$ is again integral over D, and we have $\mathrm{Tr}(x\alpha_i) = \sum_{j=1,\ldots,r} \mathrm{Tr}(x_j \gamma_j \alpha_i) = \sum_{j=1,\ldots,r} x_j \,\mathrm{Tr}(\gamma_j \alpha_i) = x_i$. Now, as the conjugates of $x\alpha_i$ are all integral over D, $\mathrm{Tr}(x\alpha_i)$ is integral over D and $x_i \in D$. □

Proposition 1.1.11. *Let D be a Dedekind domain, K its field of fractions, L a finite separable extension of K. Then the integral closure of D in L is a Dedekind domain.*

Proof. We'll call E the integral closure of D in L. The last lemma assures us E is noetherian, as all its ideals are finitely generated as D-modules, so they are a fortiori finitely generated as E-modules. E is clearly integrally closed and it has dimension 1 by the *Going-Down Theorem*. □

As a corollary, the ring of integers of any number field is a Dedekind domain. Now, observe there is an exact sequence of abelian groups:

$$1 \to D^* \to K^* \to I(D) \to \mathrm{Cl}(D) \to 1$$

For a general Dedekind domain we know little of either the group of units or the ideal class group; morover, any abelian group can be realized as the ideal class group of a Dedekind domain! Lucky for us, the situation for the ring of integers of number fields is way more tame, and we have this very strong result:

Theorem 1.1.12. *Let k be a number field. Then:*

1. *The ideal class group of $\mathcal{O}_k$ is finite.*
2. *The group of units of $\mathcal{O}_k$ is finitely generated. To be more precise, if r_1 is the number of embeddings of k into $\mathbb{R}$ and $2r_2$ is the number of embeddings of k into $\mathbb{C}$, then the group of units of $\mathcal{O}_k$ is generated by $r_1 + r_2 - 1$ elements.*

Proof. See [2]. □

1.2 Absolute values and product formulas

An extremely important instrument while studying the properties of a field is that of the norms, or absolute values, defined over that field:

Definition 1.2.1. Let K be a field. An *absolute value* v on K is a function $|.|_v : K \to \mathbb{R}^+$ such that:

1. $|ab|_v = |a|_v|b|_v$.
2. $|a+b|_v \leq |a|_v + |b|_v$.
3. $|0|_v = 0$.

   An absolute value is said to be *ultrametric* if instead of (2) it satisfies the stronger property:

4. $|a+b|_v \leq \max(|a|_v, |b|_v)$.

If K is a subfield of $\mathbb{C}$, and $\sigma : K \to \mathbb{C}$ is an embedding, the function assigning to an element of K a power (greater than or equal to one) of the usual absolute value of its image trough σ is an absolute value.

Definition 1.2.2. Any absolute value obtained this way is called an *archimedean* absolute value.

Now, let K be the fraction field of a Dedekind domain D. There is an extremely natural family of ultrametric absolute values on K:

Proposition 1.2.1. *Let K be the fraction field of a Dedekind domain D. Let P be a nonzero prime ideal of D, and v_P the discrete valuation related to the DVR D_P. For any $r > 1$, the function $k \to r^{-\mathrm{v}_P(k)}$ is an ultrametric absolute value on K.*

Proof. This is immediate from the properties of discrete valuation given in Definition (1.1.1) and those of the exponential function. □

Definition 1.2.3. If K is a number field, and thus $D = \mathcal{O}_k$, any absolute value obtained this way is called *euclidean*.

Clearly, two absolute values obtained from the same prime ideal with different bases for the exponential would yield the exact same information: we need to develop a concept of independence for absolute values. Given an absolute value, it induces a dinstance function on K in the obvious way $\mathrm{d}(a,b) = |a-b|$, thus inducing a structure of metric space on K. We may then define our concept of independence:

Definition 1.2.4. Two absolute values v_1, v_2 are *independent* if the topologies they define are different, and *dependent* otherwise.

While this sounds not so easy to check, the criterion for checking if two absolute values are dependent is actually very simple:

Proposition 1.2.2. *Let v_1, v_2 be absolute values over a field K. v_1, v_2 are dependent if and only if $|x|_{v_1} < 1 \Leftrightarrow |x|_{v_2} < 1$ for all x in K. Also, if v_1 si dependent on v_2 there is $\lambda \in \mathbb{R}^+$ such that $v_1 = {v_2}^{\lambda}$.*

Proof. First, suppose $|x|_{v_1} < 1 \Leftrightarrow |x|_{v_2} < 1$. Let x_0 be such that $|x_0|_{v_1} > 1$, this also implies $|x_0|_{v_2} > 1$. Let $\lambda = \frac{\log(|x_0|_{v_1})}{\log(|x_0|_{v_2})}$. Let now $x \in K$. There is $a \in \mathbb{R}^+$ such that $|x_0|_{v_2}^a = |x|_{v_2}$. Let $m, n \in \mathbb{N}$ such that $\frac{m}{n} > a$. We have ${|x_0|_{v_2}}^{\frac{m}{n}} > |x|_{v_2}$, so ${|x_0|_{v_2}}^m > {|x|_{v_2}}^n$ and $|\frac{{x_0}^m}{x^n}|_{v_2} < 1$ which implies $|{x_0}^{\frac{m}{n}}|_{v_2} > |x|_{v_2}$. By choosing m, n such that $\frac{m}{n} < a$ we obtain the opposite inequality, implying $|x|_{v_2} = |x_0|_2^a$. Now, as $|\frac{x_0}{x}|_{v_2} < 1$ implies the same for v_1, so does $|\frac{x_0}{x}|_{v_2} > 1$, we have $|x|_{v_1} = {|x_0|_{v_1}}^a$. This clearly implies $v_1 = {v_2}^{\lambda}$.

Conversely, if there is x such that, say, $|x|_{v_1} < 1$, $|x|_{v_2} \geq 1$ then given any surrounding of zero in the first topology it contains a positive power of x, while this is not true for the second topology, so they must be different. □

This immediately determines whenever two euclidean absolute values are dependent:

Corollary 1.2.3. *The two euclidean absolute values v_{P_1}, v_{P_2} defined by $|x|_{P_i} = {r_i}^{\mathrm{v}_{P_i}(x)}$ are dependent if and only if the ideals P_1 and P_2 are the same.*

Proof. clearly this is because the set $\{|x|_{P_i} < 1\}$ is equal to the maximal ideal of D_{P_i}. □

Now we can define what kind of sets of absolute values are good for us to use.

Definition 1.2.5. A set M of absolute values over a field K is said to be *proper* given any two values in M they are independent, and given any $x \in K$ the set of values in M such that $|x| > 1$ is finite.
A proper set of absolute values M is said to satisfy the *product formula* with multiplicities λ_v if it satisfies the equation:

$$\prod_{v \in M} {|x|_v}^{\lambda_v} = 1$$

For all $x \in K$. We'll just say it satisfies the *product formula* if $\lambda_v = 1$ for all v.

This clearly implies that M contains at most a finite number of euclidean values. Now, let's see a very important example of proper set of absolute values:

Proposition 1.2.4. *Let $v_\infty = |.|$ be the usual absolute value over $\mathbb{Q}$. For a prime number P, consider the absolute value v_P on $\mathbb{Q}$ given by $|x|_{v_P} = |P|^{\mathrm{v}_P(x)}$. Let $\{P_i\}_{i\in\mathbb{N}}$ be the set of prime numbers. The set $M_\mathbb{Q} = \{v_\infty\} \cup \{v_{P_i}\}_{i\in\mathbb{N}}$ is a proper set of absolute values over $\mathbb{Q}$, and it satisfies the product formula.*

Proof. All three properties are easily verified. □

The set $M_\mathbb{Q}$ is called the *canonical set* of $\mathbb{Q}$. Given a number field K, we want to construct a proper set of absolute values on K satisfying the product formula, somehow related to the canonical set of $\mathbb{Q}$. First we'll see how we can extend an absolute value to any algebraic extension of $\mathbb{Q}$.

Definition 1.2.6. An absolute value w over an algebraic extension L of K is said to *extend* an absolute value v on K if $w_{|K}$ is dependent on v.

There are two obvious ways of extending an archimedean or euclidean absolute value: respctively, extenending the relative embedding and taking a prime ideal that contains the old one.

Proposition 1.2.5. *Let K be a number field, and L a finite extension of K. Let v be an absolute value on K.*

- *If v is archimedean, say $|x|_v = |\phi(x)|^s$ for some embedding ϕ and exponent s, let $\psi : L \to \mathbb{C}$ be a given embedding such that $\psi_{|K} = \phi$. Clearly, there always is one. Let E be the Galois closure of L, $\sigma \in \mathrm{Gal}(E/K)$: then the absolute value v_σ given by $|x|_{v_\sigma} = |\sigma(\psi(x))|$ extends v.*
- *If v is euclidean, say $|x|_v = r^{\mathrm{v}_P(x)}$, and Q is a prime ideal appearing in the prime ideal factorization of $\mathcal{O}_L P$, the euclidean absolute value v_Q given by $|x|_{v_Q} = t^{\mathrm{v}_Q(x)}$ extends v.*

Proof. v_σ and v_Q are respectively an archimedean and an euclidean absolute value by contsruction and verifying they extend v is immediate. □

Clearly, by taking this process to the limit, one can always extend an absolute value from a number field to $\overline{\mathbb{Q}}$.

Now we construct the *canonical set* of a number field K by taking a maximal indipendent subset of all the extensions of the absolute values in $M_\mathbb{Q}$ obtained this way. To make things simpler, we may also modify all values such that restricted to $\mathbb{Q}$ they are exactly equal to the absolute value they extend.
We'll suppose at first K is a Galois extension of $\mathbb{Q}$. This immediately implies that if K is not a real field the automorphism given by sending a number to its complex conjugate does not change the usual absolute value, so we'll expect to obtain, rather than as many archimedean values as the cardinality of the Galois group of K over $\mathbb{Q}$, half that number.

Proposition 1.2.6. *Let K be a number field, and suppose $K/\mathbb{Q}$ is Galois. The set $M_{K,\infty}$ (which we'll refer to as just M_∞ if the field is clear by context) of independent absolute values extending v_∞ has cardinality equal to $[K:\mathbb{Q}]$ if K is a real field, and $\frac{1}{2}[K:\mathbb{Q}]$ otherwise.*

Proof. First, as after fixing a "canonical" embedding of K into $\mathbb{C}$ any other differs by an element of the Galois group of K over $\mathbb{Q}$, there are at most $[K:\mathbb{Q}]$ possible archimedean values on K.
Let σ_1, σ_2 two elements of the Galois group of K over $\mathbb{Q}$ which are not equal when restricted to $K \cap \mathbb{R}$. Let x be an element of K such that $\sigma_1(x) \neq \sigma_2(x)$. Suppose $\sigma_1(x) > \sigma_2(x)$: then there is $\frac{p}{q} \in \mathbb{Q}$ such that $\frac{p}{q} + \sigma_1(x) = \sigma_1(\frac{p}{q} + x) > 1$ and $\frac{p}{q} + \sigma_2(x) = \sigma_2(\frac{p}{q} + x) < 1$, thus v_{σ_1} and v_{σ_2} are independent by Proposition (1.2.2). This shows there are at least $[K \cap \mathbb{R} : \mathbb{Q}]$ different archimedean values on K. Now, if K is a complex field, the automorphism τ sending a number to its complex conjugate is an element of the Galois group of K over $\mathbb{Q}$, and all the elements of the Galois group are dependent on their composition with τ, so that there are at most $\frac{1}{2}[K:\mathbb{Q}] = [K \cap \mathbb{R} : \mathbb{Q}]$ independent archimedean values. □

We have no easy way to determine the numbers of euclidean absolute values on K exteng a P-adic value. However, for our purposes it will be sufficient to notice that the action of the Galois group is transitive.

Proposition 1.2.7. *Let L/K be a finite Galois extension of number fields, and let P be a prime ideal of $\mathcal{O}_L$. The action of the Galois group* $\mathrm{Gal}(L/K)$ *is transitive on the ideals appearing in the prime decomposition of $\langle P \rangle$.*

Proof. Let $I_1 \dots I_r = \{P\}$ be the prime ideal factorization of P. Suppose the action of the Galois group is not transitive. Then there is a subset $\{I_{r_1}, \dots, I_{r_k}\}$ fixed by $\mathrm{Gal}(L/K)$. Let $s \in I_{r_1} \setminus \cup_{r \neq r_1} I_r$. If there was $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(s) \in I_q$ with $I_q \notin \{I_{r_1}, \dots, I_{r_k}\}$ then necessarily $\sigma(I_q) = I_{r_1}$ and $\{I_{r_1}, \dots, I_{r_k}\}$ would not be invariant. Then $S = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(s)$ belongs to $I_{r_1} \dots I_{r_k}$ but not to $I_1 \dots I_r$. As S is fixed by $\mathrm{Gal}(L/K)$, it must belong to $P = I_1 \dots I_r$, which is impossible. □

Corollary 1.2.8. *Let P be a prime ideal of K. The exponents of the prime factors of P in $\mathcal{O}_L$ are all the same and the number of factors divides $[L:K]$. The euclidean absolute values extending $|.|_P$ are all conjugated by the action of the Galois group.*

Proof. These are both obvious consequences of the fact that the Galois group acts transitively. □

While this proposition is strong enough for our means, it is important to notice that it is actually a corollary of an extremely stronger, and important, theorem:

Theorem 1.2.9. *Let L/K be a Galois field extension. Let v be a absolute value over K. Let v' be an absolute value over L extending $|.|_v$. Then, another absolute value on L extends $|.|_v$ if and only if it is obtained by v by composing by an element of the Galois group of L/K.*

Proof. See [6]. □

We're ready to prove that the canonical set of K is a proper set of absolute values satisfying a product formula with fitting multiplicities.

Proposition 1.2.10. *The canonical set M_K is a proper set of absolute values on K, and there is a choice of exponents $\{\lambda_v\}_{v\in M_K}$ such that M_K satisfies the product formula with multiplicities λ_v.*

Proof. The absolute values of M_K are independent by construction. Let $x \in K$, and let $x = \frac{a}{b}$ be a representation of x as a fraction, where $a, b \in \mathcal{O}_K$ and $a \notin \langle b\rangle$. Then the euclidean norms such that $|x|_v \neq 1$ are those appearing in either the prime ideal factorization of $\langle a\rangle$ or that of $\langle b\rangle$. As those are finite in number, and there is only a finite number of archimedean values, the subset of M_K such that $|x|_v \neq 1$ is finite and thus M_K is proper.
To show it satisfies the product formula, first we suppose $K/\mathbb{Q}$ is Galois. Recall that given a finite Galois extension K/E the norm from K to E of an element $x \in K$ is ${\mathrm{N}_E}^K(x) = \prod_{\sigma\in\mathrm{Gal}(K/E)} \sigma(x)$. Clearly ${\mathrm{N}_E}^K(x) \in E$. Now, consider the product of all archimedean values of a given $x \in K$; $\prod_{v\in M_\infty} |x|_v$ is equal to:

- The product $\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} |\sigma(x)| = |\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} \sigma(x)| = |{\mathrm{N}_\mathbb{Q}}^K(x)|$ if K is a real field.
- The product $\prod_{\sigma\in\mathcal{L}\subset\mathrm{Gal}(K/\mathbb{Q})} |\sigma(x)| = |\prod_{\sigma\in\mathcal{L}\subset\mathrm{Gal}(K/\mathbb{Q})} \sigma(x)| = |{\mathrm{N}_\mathbb{Q}}^K(x)|^{\frac{1}{2}}$, where $\mathcal{L}$ is a left lateral class of the subgroup $\{\tau, \mathrm{Id}\}$ of $\mathrm{Gal}(K/\mathbb{Q})$ otherwise.

So, let λ_v be equal to 1 for all $v \in M_\infty$ if K is a real field, and 2 otherwise. Let's now consider the set M_P of euclidean values extending the P-adic value of $\mathbb{Q}$. This set is nonempty, so we randomly choose $v_0 \in M_P$. The set M_P can then be rewritten $\{v_0 \circ \sigma \mid \sigma \in \mathcal{L}\}$, where $\mathcal{L}$ is any left lateral class of the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ that fixes v_0. Let λ_P be the cardinality of this subgroup. Now:

$$\prod_{v\in M_P} |x|_v = \prod_{\sigma\in\mathcal{L}} |\sigma(x)|_v = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} |\sigma(x)|^{\frac{1}{\lambda_P}} = |{\mathrm{N}_\mathbb{Q}}^K(x)|_{v_0}{}^{\frac{1}{\lambda_P}} = |{\mathrm{N}_\mathbb{Q}}^K(x)|_{v_P}{}^{\frac{1}{\lambda_P}}.$$

It's now immediate how to conclude the proof:

$$\prod_{v\in M_K} |x|_v{}^{\lambda_v} = \prod_{v\in M_\infty} |x|_v{}^{\lambda_v} \prod_{P\in\mathrm{spec}(\mathbb{Z})} (\prod_{v\in M_P} |x|_v{}^{\lambda_v}) = \prod_{v\in M_\mathbb{Q}} |{\mathrm{N}_\mathbb{Q}}^K(x)|_v = 1.$$

Now, if K is not Galois, let L be its Galois closure. Recall every absolute value on K extends to one on L, and every absolute value on L restricts to one on K. Then choosing appropriate multiplicities γ_v we obtain, for some fixed $r \in \mathbb{N}$, $\prod_{v \in M_K} |x|_v{}^{\gamma_v} = \prod_{v \in M_L} (|x|_v{}^{\lambda_v})^r = (\prod_{v \in M_L} |x|_v{}^{\lambda_v})^r = 1$. □

Another fundamental property of the canonical set of a number field K is this:

Theorem 1.2.11. *Let K be a number field. Given any real constant $M \geq 0$, there are only finitely many $x \in K$ such that $|x|_v \geq M$ for all $v \in M_K$.*

Proof. See [2]. □

This theorem lies at the base of the possibility of counting the rational points of an algebraic variety. As our varieties will most often be projective, we would like to have a mean to determine "how big" is a given rational point of $\mathbb{P}_K{}^n$ taking into account all the canonical absolute values of K.

Definition 1.2.7. Let K be a field with a proper set of absolute values M_K satisfying the product formula with multiplicities λ_v, and let $\overline{x} = (x_1 : \ldots : x_n)$ be a K-rational point of $\mathbb{P}_K{}^n$. The *height* of $\overline{x}$ is defined by $\mathrm{H}(\overline{x}) = \prod_{v \in M_K} \max_{i=1,\ldots,n}(|x_i|_v{}^{\lambda_v})$. If $x \in K$, we define $\mathrm{H}(x) = \mathrm{H}(x : 1)$.

Proposition 1.2.12. *The height is well defined.*

Proof. First, the product makes sense as there are only finite factors different from one. Let $\overline{x} = (\gamma x_1 : \ldots : \gamma x_n)$ be another way to write $\overline{x}$, then $\mathrm{H}(\gamma x_1 : \ldots : \gamma x_n) = (\prod_{v \in M_K} |\gamma|_v{}^{\lambda_v})\,\mathrm{H}(x_1 : \ldots : x_n) = \mathrm{H}(x_1 : \ldots : x_n)$ by the product formula. □

1.3 Completions

The structure of metric space induced on a field by an absolute value still lacks some important properties, the most evident one being completeness. In this section we'll show how to extend our base field and our absolute value to make the induced metric complete and, in the case of number fields, locally compact. To do this, as one would expect, we'll proceed as for any other metric space using the Cauchy sequences, with the only difference we'll have to prove the obtained space is a field. First we'll show the field operation are continuous with respect to the v-adic topology:

Proposition 1.3.1. *The sum, product and inverse are continuous with respect to the v-adic topology.*

Proof. Clearly $K \times K$ is equipped with the product topology, which is induced by the norm $|(x,y)|_v = \max(|x|_v, |y|_v)$. Now, to prove the sum is continuous we just need to show that if $(x_n, y_n)_{n\in\mathbb{N}} \to (a,b)$, the sequence $(x_n + y_n)_{n\in\mathbb{N}}$ has $a+b$ as a limit. This is obvious as $|x_n + y_n - a - b|_v \leq |x_n - a|_v + |y_n - b|_v$.
To prove the product is continuous, let again $(x_n, y_n)_{n\in\mathbb{N}} \to (a,b)$, then let $a_n = x_n - a, b_n = x_n - b$. We have $|x_n y_n - ab|_v = |ab - ab + a_n b_n + x_n b_n + y_n a_n|_v = |a_n b_n + x_n b_n + y_n a_n|_v$. As x_n and y_n are bounded this sequence has 0 as a limit.
Let now $x_n \to a$. Then $|{x_n}^{-1} - a^{-1}|_v = |\frac{x_n - a}{x_n a}|_v = |x_n - a|_v |x_n a|_v{}^{-1}$. As $|x_n a|_v \to |a|_v{}^2$ by the continuity of the product and $|x_n - a|_v \to 0$ by the continuity of the product, $|{x_n}^{-1} - a^{-1}|_v \to 0$ and the inverse is continuous. □

Consequently, all rational functions are also continuous with respect to the v-adic topology.

Definition 1.3.1. Let K be a field and v an absolute value on K. A sequence $(x_n)_{n\in\mathbb{N}}$ is a *Cauchy sequence* with respect to the v-adic if for all $\epsilon > 0$ there is $N \in \mathbb{N}$ such that $|x_r - x_s|_v < \epsilon$ for all $r, s \geq N$.

Definition 1.3.2. The completion K_v of K with respect to the v-adic topology is the set of Caucy sequences quotiented by the relation $(x_n)_{n\in\mathbb{N}} \sim (y_m)_{m\in\mathbb{N}}$ if for all $\epsilon > 0$ there is $N \in \mathbb{N}$ such that $|x_n - y_m|_v < \epsilon$ for all $n, m \geq N$. There is a natural inclusion $K \in K_v$ given by sending $x \in K$ to the Cauchy sequence assuming x as its only value.

This is the usual procedure to construct the completion of a metric space, and thus we'll give for granted the reader knows K_v is a complete metric space when equipped with the distance given by $\mathrm{d}_v((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) = \lim(|x_n - y_n|_v)$. What we have to show is that K_v is a field and the norm induced by this distance is an absolute value on K_v.

Proposition 1.3.2. *K_v can be given a field structure, the inclusion of K is an embedding and the absolute value v can be extended to K_v.*

Proof. We define the sum, product and inverse respectively as:

- $(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}}$.
- $(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} = (x_n y_n)_{n\in\mathbb{N}}$.
- $(x_n)_{n\in\mathbb{N}}{}^{-1} = ({x_n}^{-1})_{n\in\mathbb{N}}$.

Using the continuity of field operations it is trivial to check these operations are well defined and they respect all the field properties. We now define the absolute value v on K_v by setting:

- $|(x_n)_{n\in\mathbb{N}}|_v = \lim(|x_n|_v)$

This is well defined as $(|x_n|_v)_{n\in\mathbb{N}}$ is a Cauchy sequence of $\mathbb{R}$, and all properties of absolute values are respected again thanks to the continuity of field operations. □

A field is said to be *complete* with respect to an absolute value v if the inclusion into its v-adic completion is surjective. An example which is immediately treatable is $\mathbb{Q}$ with the usual absolute value. As one immediately sees, its completion is $\mathbb{R}$.
As finite field extensions are finite vector space over their base field, it's quite easy to guess how completions interact with finite extensions:

Proposition 1.3.3. *Let K be a field, v an absolute value on K, L a finite algebraic extension of K, and w an absolute value on L extending v. Then E_w is isomorphic to the composite field EK_v as a K_v-algebra, and the absolute value w on E_w extends v on K_v.*

Proof. See [6]. □

This also implies the completion of a number field with respect to an archimedean absolute value is always either $\mathbb{R}$ or $\mathbb{C}$. There is one last property we need to enounce:

Proposition 1.3.4. *Let K be a number field, $v \in M_K$. Then K_v is locally compact with respect to the v-adic topology.*

Proof. See [7]. □

1.4 Normal and regular varieties

We'll need some basic algebraic geometry troughout this dissertation. Our language will be that of schemes theory, and we'll suppose the reader had a basic course on the subject, and thus is accustomed to the concepts of scheme, open and closed immersions, reduced, integral, locally noetherian and noetherian schemes, fibered product, separated morphisms, proper and projective morphisms. While most of the theorems we'll use will hold for any reasonable (noetherian) scheme, our main object of interest will be *algebraic varieties*. For a more complete and general treatment of the subject, see [3].

Definition 1.4.1. Let k be a field. An *Algebraic Variety* X over k is a separated, reduced k-scheme such that the structural morphism $X \to \text{spec}(k)$ is of finite type. An algebraic variety is said to be *Projective* if $X \to \text{spec}(k)$ is projective, which also implies it is of finite type and separated.

Normality and regularity are fundamental conditions for most results while working with algebraic varieties. Both are local properties, meaning they are properties of the stalks, and thus can be verified on an affine covering, and pass on to open subschemes.

Definition 1.4.2. Let X be an integral, noetherian scheme. X is said to be:

- Normal at a point p, if the stalk $\mathcal{O}_{X,p}$ is integrally closed. X is normal if it is normal at all of its points.
- Regular at a point p, if the stalk $\mathcal{O}_{X,p}$ is regular. X is regular if it is regular at all of its points.

Regular schemes are always normal, as implied by this fundamental result in local algebra:

Theorem 1.4.1. *Let A be a local regular noetherian ring. The following properties hold:*

- *for all $p \in \text{spec}(A)$, A_p is regular.*
- *A is a unique factorization domain.*

As any UFD is integrally closed, this implies a regular scheme is also normal. The only case where the two definiton are equivalent is the 1-dimensional case:

Proposition 1.4.2. *Let X be a normal scheme of dimension 1. Then X is regular.*

Proof. Given any point $p \in X$, the stalk $\mathcal{O}_{X,p}$ has dimension at most one: if the dimension is 0 then $\mathcal{O}_{X,p}$ is a field and thus regular, and if the dimension is 1 by Proposition (1.1.2) $\mathcal{O}_{X,p}$ is a DVR, and thus regular. □

Normal schemes gives us powerful tools to work with, such as the following extension theorem:

Theorem 1.4.3. *Let X be a normal S-scheme, Y a proper S-scheme. Let U be a nonemepty open subset of X, and $f : U \to Y$. Then f can be extended to a morphism $f : V \to Y$, where V is an open subset of X containing all points of codimension ≤ 1.*

Proof. See [3]. □

Given a scheme X, it is often convenient to consider a "normal model" for X, which we call the *normalization* of X.

Definition 1.4.3. Let X be an integral noetherian scheme. A pair (Y, π), where Y is a scheme and $\pi : Y \to X$ is a *normalization* of X if it is normal and every dominant morphism from a normal scheme to X factors trought π. Note that if U is an open subscheme of X, $(\pi^{-1}(U), \pi_{|\pi^{-1}(U)})$ is a normalization of U.

The existence of a normalizion is quite intuitive for affine schemes:

Lemma 1.4.4. *Let A be an integral domain, and B an integrally closed integral domain. Then any injective morphism $f : A \to B$ factors uniquely trought the immersion of A into its integral closure.*

Proof. As the subfield $\mathrm{Frac}(f(A))$ of $\mathrm{Frac}(B)$ is isomorphic to $\mathrm{Frac}(A)$, the natural map $\tilde{f} : \mathrm{Frac}(A) \to \mathrm{Frac}(B)$ sends the integral closure of A to a subring of B, and thus f factors as the immersion of A into its integral closure composed by $\tilde{f}$. As $\tilde{f}$ is determined by f, the factorization is unique. □

Proposition 1.4.5. *Let $X \doteq \mathrm{spec}(A)$ be an affine scheme, and let A^ν be the integral closure of A: then the pair $(\mathrm{spec}(A^\nu) \doteq X^\nu, \pi)$, where π is the morphism induced by the immersion of A into A^ν is a normalization of X.*

Proof. Given an affine scheme X, any morphsim $f : Y \to X$ is induced by the morphism of rings $f^\sharp : \mathcal{O}_X(X) \to \mathcal{O}_Y(Y)$, thus the (unique) factorization implied by the last lemma induces a corresponding unique factorization $f = \tilde{f} \circ \pi$. □

Once we know the normalizion exists for affine schemes, we can define it in general by glueing:

Proposition 1.4.6. *Let X be an integral, noetherian scheme: then the normalization (X^ν, π) exists and is unique up to isomorphism of X-schemes. Moreover, any pair (Y, f) such that Y is normal and f is birational and integral (that is, for every affine subset U of X $f^{-1}(U)$ is affine and $f^\sharp_{|U}$ is integral) is a normalization of X.*

Proof. The uniqueness of the normalization is immediate, as for all objects defined by a universal property. To prove the existence, consider an affine covering $\{X_i\}_{i=1,\dots,r}$ of X. As the normalization of $X_i \cap X_j$ exists (it is the open subscheme $\pi^{-1}(X_i \cap X_j)$ of X_i^ν) and is unique, we may glue the ${X_i}^\nu$ along those open subschemes, obtaining a normalization (X^ν, π) of X.
Suppose now we have a pair (Y, f) satisfying the conditions above: then given an affine open subscheme U of X, consider the morphism $f^\sharp : \mathcal{O}_X(U) \to \mathcal{O}_Y(f^{-1}(U))$. As f is birational we have $K(Y) = f^\sharp K(X)$, and as f is integral, $\mathcal{O}_Y(f^{-1}(U))$ must be contained in the integral closure of $f^\sharp(\mathcal{O}_X(U))$ in $K(Y)$, thus in the image of the integral closure of $\mathcal{O}_X(U)$; as Y is normal $\mathcal{O}_Y(f^{-1}(U))$ must contain the image of the integral closure of $\mathcal{O}_X(U)$. As the map is birational, it is dominant and $f^\sharp$ is injective. Then $\mathcal{O}_Y(f^{-1}(U))$ is isomorphic to the integral closure of $\mathcal{O}_X(U)$, and by choosing an affine covering and glueing we obtain that Y is isomorphic to X, and the isomorphism sends f to the projection π. □

Notice that it is not generally true for the normalization to be a birational morphism. This is true when the normalization morphism is finite.

Proposition 1.4.7. *Let X be a scheme such that the normalization morphism $X^\nu \to X$ is finite. Then the set of X^{norm} of points p such that X is normal at p is open.*

Proof. It suffices to show it for affine schemes. Let A be an integral domain, A^ν its integral closure. As the normalization morphism is finite, A^ν is finite as an A-module. $\mathrm{spec}(A)$ is normal at a point p if and only if ${A^\nu}_{/A_p} = ({A^\nu}_{/A})_p = 0$; consider the ideal $\mathrm{Ann}({A^\nu}_{/A})$ of A: if p belongs to $\mathrm{spec}(A) \setminus \mathrm{V}(\mathrm{Ann}({A^\nu}_{/A}))$, then there is $a \in \mathrm{Ann}({A^\nu}_{/A})$ in $A \setminus p$, which implies $({A^\nu}_{/A})_p = 0$. Conversely, as ${A^\nu}_{/A}$ is finite as an A module, if its localization at p is 0 given a set of generators $e_1, \dots, e_r$ of ${A^\nu}_{/A}$ there are $a_1, \dots, a_r$ in $A \setminus p$ such that $a_i e_i = 0$. As the e_i are finite, we may take the product $a_1 \dots a_r \in \mathrm{Ann}({A^\nu}_{/A}) \cap (A \setminus p)$, which implies $p \in \mathrm{spec}(A) \setminus \mathrm{V}(\mathrm{Ann}({A^\nu}_{/A}))$. □

Clearly, if this happens, the normalization morphism restricted to X^{norm} is an isomorphism and thus it is birational. As one would expect from classical examples, a class of schemes such that the normalization morphism is finite, and thus birational, is that of algebraic varieties.

Proposition 1.4.8. *Let X be an algebraic variety over a perfect field k. Then the normalization morphsim $\pi : X^\nu \to X$ is finite.*

Proof. It suffices to prove it for affine varieties. Recall by *Noether's Normalization Lemma* there are $f_1, \ldots, f_r \in \mathcal{O}_X(X)$ such that $f_1, \ldots, f_r$ are algebraically independ over k and $K(X)$ is finite over $k(f_1, \ldots, f_r)$. Then the integral closure of $\mathcal{O}_X(X)$ in $K(X)$ is the same as that of $k[f_1, \ldots f_r]$; as $k[f_1, \ldots f_r]$ is integrally closed and $K(X)$ is a finite separable extension of $k(f_1, \ldots, f_r)$, we may apply (1.1.10), obtaining that $(\mathcal{O}_X(X))^\nu$ is finite over $k[f_1, \ldots f_r]$, and thus over $\mathcal{O}_X(X)$. □

This implies an extremely important property of normalizations:

Proposition 1.4.9. *The normalization of an algebraic variety over a perfect field k is an algebraic variety over k.*

Proof. Let X be an algebraic variety over k, and X^ν its normalization. As X^ν is finite over X, it is of finite type over k. As X^ν is normal, it is clearly reduced. As for separatedness, any affine morphism (a morphism such that the pre-image of an affine open subset is affine) is separated, and the composition of two separated morphisms is separated. □

1.5 $\mathcal{O}_X$-modules and invertible sheaves

As modules are fundamental in the study of rings, the concept of $\mathcal{O}_X$-module is a fundamental tool in scheme theory, and a basic step for most significative results.

Definition 1.5.1. Let $(X, \mathcal{O}_X)$ be a ringed space. A *sheaf of $\mathcal{O}_X$-modules* $\mathcal{F}$ is a sheaf of abelian groups on X such that for any open set U $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module, and the morphisms $\rho_{U,V}$ are morphisms of $\mathcal{O}_X(U)$-modules.

As for schemes, the most basic shaves of $\mathcal{O}_X$-modules are directly obtained by their algebraic counterparts:

Definition 1.5.2. Let A be a ring, and M an A-module. For any principal open subset of $\mathrm{Spec}(A)$ $U \doteq \mathrm{D}(f)$ consider the $\mathcal{O}_{\mathrm{spec}(A)}(U)$-module M_f, and given any other principal subset $V \doteq \mathrm{D}(g)$ let $\rho_{U,V}$ be the natural map $M_f \to M_{fg}$. This defines a unique structure of sheaf of $\mathcal{O}_{\mathrm{spec}(A)}$-modules, which we'll call $\tilde{M}$.

We'd like these "affine" shaves of $\mathcal{O}_X$-modules to be the building bricks of our theory. It's easy to see our definition of a sheaf of $\mathcal{O}_X$-modules is not strong enough to assure this even for affine schemes, so we'll generally restrict to a subcategory, that of *Quasi-coherent shaves*.

Definition 1.5.3. A sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is said to be *Quasi-coherent* if there is an affine covering $\{U_i\}_{i\in I}$ of X such that for all $i \in I$ there is an $\mathcal{O}_X(U_i)$-module M_i satisfying $\mathcal{F}_{|U_i} \simeq \tilde{M}_i$. A sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is said to be *Coherent* if it is *Quasi-coherent* and X is noetherian.

For brevity, we'll just call them *Quasi-coherent sheaves* and *Coherent sheaves*. Morphsims, direct sums, direct products and tensor products of sheaves of $\mathcal{O}_X$-modules are defined as usual. Let us see some basic properties regarding the sheaves $\tilde{M}$:

Proposition 1.5.1. *Let $X = \mathrm{spec}(A)$ be an affine scheme. the following properties hold:*

1. $(\tilde{\oplus_{i\in I}} M_i) = \oplus_{i\in I} \tilde{M}_i$.
2. $(M \tilde{\otimes}_A N) = \tilde{M} \otimes_{\mathcal{O}_{\mathrm{spec}(A)}} \tilde{N}$.
3. *A sequence of sheaves of $\mathcal{O}_{\mathrm{spec}(A)}$-modules $\tilde{L} \to \tilde{M} \to \tilde{N}$ is exact if and only if the sequence $L \to M \to N$ is exact.*
4. *Let $f : \tilde{M} \to \tilde{N}$ be a morphism of $\mathcal{O}_X$-modules. Then f is the morphism induced by $f_X : \tilde{M}(X) = M \to \tilde{N}(X) = N$.*

Proof. See [3]. □

The definition of Quasi-coherent sheaves does not imply that for a Quasi coherent sheaf $\mathcal{F}$ given any affine open subset $U = \text{spec}(A)$ the equality $\mathcal{F}_{|U} \simeq \mathcal{F}\tilde{(U)}$. Luckily, this can be shown to be true:

Theorem 1.5.2. *Let $\mathcal{F}$ be a Quasi-coherent sheaf on a scheme X, and let U be an affine open subset of X. Then $\mathcal{F}_{|U} \simeq \mathcal{F}\tilde{(U)}$.*

Proof. See [3]. □

This allows us to show the first example of a sheaf of $\mathcal{O}_X$-modules that is not Quasi-coherent:

Example 1.5.4. Let $X = \text{spec}(A)$ be an affine scheme, I an ideal of A. Consider I as an A-module. Let m be a maximal of A, and let $\mathcal{F}_i = \tilde{m^i}$. Clearly $\mathcal{F}_i \subset \mathcal{F}_{i-r}$ is a subsheaf of $\mathcal{O}_X$-modules. We can then define $\mathcal{F} = \cap_{i\in\mathbb{N}}\mathcal{F}_i$. Clearly $\mathcal{F}$ is a sheaf of $\mathcal{O}_X$-modules. For an open subset U of X, we have:

- $\mathcal{F}(U) = 0$ if $m \in U$.
- $\mathcal{F}(U) = \mathcal{O}_X(U)$ if $m \notin U$.

Then $\mathcal{F}$ is not quasi-coherent, as $\mathcal{F}(X) = 0$, which would imply by last theorem $\mathcal{F}(U) = \tilde{0}(U) = 0$ for all U.

We can now show that the subcategory of Quasi-coherent sheaves is stable by the usual (finite) operations of sheaves:

Proposition 1.5.3. *the following properties are true:*

- *A finite direct sum of Quasi-coherent (resp. Coherent) sheaves is Quasi-coherent (resp. Coherent).*
- *If $\mathcal{F}$, $\mathcal{G}$ are Quasi-coherent (resp. Coherent) sheaves on a scheme X the tensor product $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is Quasi-coherent (resp. Coherent).*
- *If $f : \mathcal{F} \to \mathcal{G}$ is a morphism of Quasi-coherent (resp. Coherent) sheaves on a scheme X the sheaves of $\mathcal{O}_X$-modules* $\text{Ker}(f)$, $\text{coker}(f)$ *and* $\text{Im}(f)$ *are Quasi-coherent (resp. Coherent).*

Proof. Choose on an affine covering of X: By Theorem (1.5.2) we may verify all these properties on this covering, and this is immediate thanks to Proposition (1.5.1). □

Direct products do not behave well with Quasi-coherent sheaves, as shown by the following example:

Example 1.5.5. Let $X = \mathbb{A}^1{}_k$, $\mathcal{F} = \mathcal{O}_X$. Then $\prod_{i\in\mathbb{N}} \mathcal{F}$ is not a Quasi-coherent. If it was Quasi-coherent, it would be isomorphic to $(\widetilde{\prod_{i\in\mathbb{N}} \mathcal{F}})(X) = \widetilde{\prod_{i\in\mathbb{N}} k}\,[t]$; this is not true as $(\frac{1}{t}, \frac{1}{t^2}, \frac{1}{t^3}, \ldots)$ belongs to $\prod_{i\in\mathbb{N}} \mathcal{F})(\mathrm{D}(t))$, but it doesn't belong to $\widetilde{\prod_{i\in\mathbb{N}} k}\,[t](\mathrm{D}(t))$.

An important object of study regarding sheaves of $\mathcal{O}_X$-modules are their *global sections*.

Definition 1.5.6. Let X be a scheme, $\mathcal{F}$ a sheaf of $\mathcal{O}_X$-modules. A *global section* s of $\mathcal{F}$ is an element of $\mathcal{F}(X)$.

- $\mathcal{F}$ is said to be *globally generated* if there is a set $\{s_i\}_{i\in I}$ of global section such that for all open subsets U there is a subset I_U of I such that $\mathcal{F}(U)$ is generated by $\{s_{i|U}\}_{i\in I_U}$.
- A set of global sections $\{s_i\}_{i\in I}$ is said to *never vanish* on X if given any point $p \in X$ there is always $j \in I$ such that $s_j \neq 0$ in $\mathcal{F}_p \otimes_{\mathcal{O}_{X,p}} K_p$.

We'll name $s(p)$ the residue class of s at apoint p as defined above. As for schemes, we may consider the subset of X where s does not vanish:

Proposition 1.5.4. *Let X be a scheme, $\mathcal{F}$ a coherent sheaf of $\mathcal{O}_X$-modules and $s \in \mathcal{F}(X)$. The set $\mathrm{D}(s) = \{p \in X \mid s(p) \neq 0\}$ is open.*

Proof. It suffices to show $U \cap \mathrm{D}(s)$ is open for any affine subset U. The $\mathcal{O}_X(U)$-module generated by s is of rank one, which implies it is isomorphic to $a^{\mathcal{O}_X(U)}\!/_I$ for some ideal I and element p. Then s vanishes at $p \in U$ whenever a does, so that $\mathrm{D}(s) \cap U = U \setminus V(a)$, which is open. □

Given a morphism of schemes $f : X \to Y$, we naturally want to construct a *pushforward* operator f_* sending sheaves of $\mathcal{O}_X$-modules to sheaves of $\mathcal{O}_Y$-modules and a *pullback* operator sending sheaves of $\mathcal{O}_Y$-modules to sheaves of $\mathcal{O}_X$-modules:

Definition 1.5.7. Let $f : X \to Y$ be a morphism of schemes.

- If $\mathcal{F}$ is a sheaf of $\mathcal{O}_X$-modules, the *pushforward* $f_*\mathcal{F}$ is the sheaf of $\mathcal{O}_Y$-modules given by $f_*\mathcal{F}(U) = \mathcal{F}(f^{-1}(U))$ with the structure of $\mathcal{O}_X(U)$-module given by $f^\sharp{}_U$ and restriction morphisms $\rho_{U,V} \doteq \rho_{f^{-1}(U),f^{-1}(V)}$.
- If $\mathcal{G}$ is a sheaf of $\mathcal{O}_Y$-modules. Recall $f^\sharp$ induces a morphsim of sheaves $f^{-1}(\mathcal{O}_Y) \to \mathcal{O}_X$, where $f^{-1}(\mathcal{H})$ is the sheaf defined by $f^{-1}(\mathcal{H})_p = \mathcal{O}_{Y\,f(p)}$. the *pullback* $f^*\mathcal{G}$ is the sheaf of $\mathcal{O}_X$-modules $f^{-1}(\mathcal{G}) \otimes_{f^{-1}(\mathcal{O}_Y)} \mathcal{O}_X$.

The pullback operator behaves well with respect to Coherent and Quasi coherent sheaves, globally generated sheaves and the vanishing set of global sections:

Proposition 1.5.5. *The pullback of a Quasi-coherent (resp.Coherent) sheaf is Quasi-coherent (resp.Coherent). The pullback of a globally generated sheaf is globally generated. Also,* $f^{-1}(D(s)) = D(f^*(s))$.

Proof. We may restrict to affine schemes. Let $X = \text{spec}(B)$, $Y = \text{spec}(A)$, $\mathcal{F} = \tilde{M}$. If $M = A^r$ the assertion is obvious as $f^*\mathcal{O}_Y = \mathcal{O}_X$ and the tensor product commutes with finite sums. If M is not free, we have an exact sequence of A-modules $N \to L \to M \to 0$ with N, L free. This gives rise to an exact sequence of sheaves of $\mathcal{O}_Y$-modules $\tilde{N} \to \tilde{L} \to \tilde{M} \to 0$; by the right exactness of the tensor product this in turn gives rise to an exact sequence $f^*\tilde{N} \to f^*\tilde{L} \to f^*\tilde{M} \to 0$. As $f^*\tilde{N}$ and $f^*\tilde{L}$ are Quasi-coherent, say $f^*\tilde{N} = \tilde{N'}$, $f^*\tilde{L} = \tilde{L'}$ it is easy to verify that $f^*\tilde{M} = \text{coker}(\tilde{N'} \to L')$. The second assertion comes directly from the right exactness of the tensor product. The third assertion is obvious. □

As we'll see in the following example, the pushforward operator may behave quite badly if we don't take some basic precaution.

Example 1.5.8. Let X be a scheme, $Y = \sqcup_{i\in\mathbb{N}} X$. Let $f : Y \to X$ be the projection sendig each copy of X isomorphically to X. Then $f_*\mathcal{O}_Y = \prod_{i\in\mathbb{N}} \mathcal{O}_X$. As we've seen, this is generally not a Quasi-coherent sheaf.

Actually,this problem of compactness is basically the main obstruction to the pushforward being Quasi-choerent:

Proposition 1.5.6. *Let $\mathcal{F}$ be a Quasi-coherent sheaf on a scheme X. Let $f : X \to Y$ be a morphism. If X is noetherian, or f is separated and Quasi-compact, then $f_*\mathcal{F}$ is Quasi-coherent on Y.*

Proof. See [3]. □

An important notion is that of *Locally free sheaf*:

Definition 1.5.9. A sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is said to be *Locally free* if there is an affine covering $\{X_i\}_{i\in I}$ of X such that $\mathcal{F}_{|X_i} \simeq \tilde{M}_i$ with M_i a free finite $\mathcal{O}_X(X_i)$-module.

Locally free sheaves are clearly Quasi-coherent, and coherent on a noetherian scheme.

Definition 1.5.10. The *Rank* of a Quasi-coherent sheaf $\mathcal{F}$ at a point $P \in X$ is the rank of $\mathcal{F}_p$ as an $\mathcal{O}_{X,p}$ module.

Clearly for a locally free sheaf $\mathcal{F}$ the rank is constant on irreducible components of X, and we can define the rank of $\mathcal{F}$ on an irreducible scheme to be the rank at any point of X. A hugely important class of sheaves of $\mathcal{O}_X$-modules is that of *invertible sheaves*.

Definition 1.5.11. A sheaf of $\mathcal{O}_X$-modules is said to be invertible if there is an affine covering $\{X_i\}_{i\in I}$ of X such that $\mathcal{F}_{|X_i} \simeq \mathcal{O}_{X_i}$ for all i, i.e. $\mathcal{F}$ is a locally free sheaf of rank one.

$\mathcal{O}_X$ is clearly an invertible sheaf. To show a large class of invertible sheaves we'll use a fundamental construction in algebraic geometry, extending the construction of $\tilde{M}$ we did for affine schemes to projective schemes. Recall that given an homogeneous element f of a graded ring A, $\mathrm{V}_+(f)$ is the set of points $p \in \mathrm{proj}(A)$ such that $(A_p f)_0 \subseteq A_p p$. $\mathrm{D}_+(f)$ is $\mathrm{proj}(A)\setminus \mathrm{V}_+(f)$.

Definition 1.5.12. Let A be a graded ring and M a graded A-module. Let $X = \mathrm{Proj}(A)$. For any principal open subset $U = \mathrm{D}_+(f)$ of X, let $\tilde{M}(U)$ be the the $A_{(f)}$ module $\{s \in M_f \mid \deg(s) = 0\}$. This defines a unique structure of (Quasi-coherent) $\mathcal{O}_{\mathrm{Proj}(A)}$-module, which we'll call $\tilde{M}$.

It can be shown that any coherent sheaf on $\mathrm{proj}(A)$ can be obtained this way. We state without proof an extremely important finiteness theorem regarding coherent sheaves on projective schemes:

Theorem 1.5.7. *Let X be a projective* $\mathrm{spec}(A)$*-scheme, with A noetherian. Then, given any coherent sheaf $\mathcal{F}$ on X, $\mathcal{F}(X)$ is a finite A-module.*

Proof. See [3]. □

Now, given a graded ring A, we consider the graded A-module $A(d)$ obtained shifting the graduation on A by d, that is, $A(d)_r = A_{r-d}$. This is called the *d-twist* of A. $\tilde{A(d)}$ is a sheaf of $\mathcal{O}_{\mathrm{proj}(A)}$-modules we'll call $\mathcal{O}_{\mathrm{proj}(A)}(d)$. As we're about to see, in the case of $A = R[x_0, \ldots, x_n]$ with the standard graduation (so that $\mathrm{proj}(A) = \mathbb{P}^n{}_R$), this is an invertible sheaf.

Proposition 1.5.8. *Let R be a ring. For all $d \in \mathbb{Z}$, $\mathcal{O}_{\mathbb{P}^n{}_R}(d)$ is an invertible sheaf.*

Proof. Let $U = \mathbb{P}^n{}_{R(x_i)}$. Then $\mathcal{O}_{\mathbb{P}^n{}_R}(d)(U) = R[x_0, \ldots, x_n](d)_{(x_i)}$ is the $\mathcal{O}_{\mathbb{P}^n{}_R}(U)$ module of all fractions $\frac{f}{{x_i}^r}$, with $f \in R[x_0, \ldots, x_n]$ homogeneous and $r = \deg(f) - 1$. This is generated by ${x_i}^d$ as an $\mathcal{O}_{\mathbb{P}^n{}_R}(U)$-module. As x_i is not a zero divisor in $R[x_0, \ldots, x_n]$, $\mathcal{O}_{\mathbb{P}^n{}_R}(d)(U)$ is isomorphic to $\mathcal{O}_{\mathbb{P}^n{}_R}(U)$, and as $\mathcal{O}_{\mathbb{P}^n{}_R}(d)$ is Quasi-coherent and U affine this implies $\mathcal{O}_{\mathbb{P}^n{}_R}(d)_{|U} \simeq \mathcal{O}_{\mathbb{P}^n{}_R}(d)_{|U}$. □

Clearly, the global sections of $\mathcal{O}_{\mathbb{P}^n{}_R}(d)$ are exactly the homogeneous polynomials of degree d in $R[x_0, \ldots, x_n]$ and 0 (which reduce to only 0 if $d < 0$), and thus are a free R-module of rank $\binom{d}{n+1}$.

The reason we call locally free sheaves of rank one invertible is that we can give the subcategory of invertible sheaves on a scheme X the structure of an abelian group, with sum given by the tensor product and identity given by $\mathcal{O}_X$. Let's do this by steps:

Definition 1.5.13. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. The *Dual sheaf* $\mathcal{F}^{\mathrm{v}}$ is the sheaf of $\mathcal{O}_X$-modules defined by $\mathcal{F}^{\mathrm{v}}(U) = \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{F}_{|U}, \mathcal{O}_U)$, with restriction maps the natural restriction of morphisms.

Proposition 1.5.9. *The following properties are true:*

- *If $\mathcal{F}$ is Quasi-coherent (resp.coherent) so is $\mathcal{F}^{\mathrm{v}}$.*
- *If $\mathcal{F}$ is locally free of rank r so is $\mathcal{F}^{\mathrm{v}}$.*

Proof. Given any affine open subset U Proposition (1.5.3) implies that $\mathcal{F}^{\mathrm{v}}(U) = \mathrm{Hom}_{\mathcal{O}_X(U)}(\widetilde{\mathcal{F}(U)}, \mathcal{O}(U))$; this in turn implies that ${\mathcal{F}^{\mathrm{v}}}_U(V)$ is isomorphic to $\mathrm{Hom}_{\mathcal{O}_X(U)}(\mathcal{F}(U), \mathcal{O}(U))(V)$ for all principal open subsets of U. As these form a base for the topology of U the two are isomorphic. The second property is an obvious consequence of the fact that $\mathrm{Hom}_A(A^r, A) \simeq A^r$. □

Proposition 1.5.10. *The tensor product of invertible sheaves is invertible, and $\mathcal{F} \otimes \mathcal{F}^{\mathrm{v}} \simeq \mathcal{O}_X$.*

Proof. The first assertion is obvious. To prove the second assertion, consider the morphism $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{F}^{\mathrm{v}} \simeq \mathcal{O}_X$ defined on any open subset U by $f \otimes \phi \to \phi(f)$ and extended by linearity. This is clearly a morphism of sheaves of $\mathcal{O}_X$-modules, and we can check surjectivity and injectivity locally, using the fact that on a stalk $(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{F}^{\mathrm{v}})_p$ the morphism restricts to $\mathcal{F}_p \otimes_{\mathcal{O}_{X,p}} ({\mathcal{F}^{\mathrm{v}}}_p = \mathrm{Hom}_{\mathcal{O}_{X,p}}(\mathcal{F}_p, \mathcal{O}_{X,p}))$ defined by $f \otimes \phi \to \phi(f)$. □

Conversely, given an invertible sheaf $\mathcal{G}$ such that $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} \simeq \mathcal{O}_X$ we can use the isomorphism to identify $\mathcal{G}$ with $\mathcal{F}^{\mathrm{v}}$. We have all the intstruments to define the *Picard Group*.

Definition 1.5.14. Let X be a scheme. The set of classes of isomorphism of invertible sheaves on X, equipped with the operation $[\mathcal{F}] + [\mathcal{G}] = [\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}]$ is an abelian group with identity $[\mathcal{O}_X]$ and inverse $-[\mathcal{F}] = [\mathcal{F}^{\mathrm{v}}]$. We call it the *Picard Group* $\mathrm{Pic}(X)$ of X.

The pullback operator is behaves well with respect to the picard group:

Proposition 1.5.11. *Let $f : X \to Y$ be a morphism of schemes. Then $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ is a morphism of abelian groups.*

Proof. This stems from the properties of tensor products and the fact that $f^*\mathcal{O}_Y = \mathcal{O}_X$. □

Given a $\mathrm{spec}(A)$-scheme X invertible sheaves allow us to classify the set $\mathrm{Hom}_{\mathrm{spec}(A)}(X, {\mathbb{P}^n}_A)$. The basic idea is that giving a morphism $f : X \to {\mathbb{P}^n}_A$ is tantamount to choosing the pullback of $\mathcal{O}_{{\mathbb{P}^n}_A}(1)$.

Proposition 1.5.12. *Let X be an A-scheme. There is bijective correspondence beetween morphisms $X \to {\mathbb{P}^n}_A$ and pairs $(\mathcal{F}, (s_0, \dots, s_n)$ where $\mathcal{F}$ is an invertible sheaf on X and $(s_0, \dots, s_n)$ an $n+1$-uple of global sections that never vanish.*

Proof. Clearly, given a morphism $X \to {\mathbb{P}^n}_A$ the sheaf $f^*\mathcal{O}_{{\mathbb{P}^n}_A}(1)$ is invertible and $(f^*x_0, \dots, f^*x_n)$ is a never vanishing $n+1$-uple of global sections. Conversely, suppose we have $(\mathcal{F}, (s_0, \dots, s_n)$ as above, let $U = \mathrm{D}(s_i)$, and let $\{U_j\}_{j\in J}$ be an affine open covering of U. let $\lambda_j : \mathcal{F}_{|U_j} \to \mathcal{O}_{U_j}$ be an isomorphism. Then $\lambda(s_{i|V})$ is invertible for all open subset V of U. Consider the morphism $V \to {\mathbb{P}^n}_{A x_i}$ induced by $\frac{x_r}{x_i} \to \frac{\lambda(s_r)}{\lambda(s_i)}_V$. This does not depend on λ, as given a generator g of $\mathcal{F}(V)$ as an ${\mathbb{P}^n}_A(V)$-module, $s_{r|V} = \alpha g$, $s_{i|V} = \beta g$ with α, β in ${\mathbb{P}^n}_A(V)$, so that $\frac{\lambda(s_r)}{\lambda(s_i)}_V = \frac{\alpha}{\beta}$ indipendently from λ. Then the morphisms we defined on the U_j glue to a morphism $U \to {\mathbb{P}^n}_{A x_i}$. By repeating this procedure for $i = 1 \dots n+1$ and glueing as before we obtain a morphism $X \to {\mathbb{P}^n}_A$ such that $f^*\mathcal{O}_{{\mathbb{P}^n}_A} = \mathcal{F}$ and $f^*x_i = s_i$. □

By using Quasi-coherent sheaves, we can define the algebraic equivalent to the usual degree of a finite morphism; first we'll define a degree for Quasi-coherent sheaves.

Definition 1.5.15. Let $\mathcal{F}$ be a Quasi-coherent sheaf on an integral scheme X. The *degree* $\deg(\mathcal{F})$ of $\mathcal{F}$ is the rank of $\mathcal{F}_\xi$ as a $\mathcal{O}_{X,\xi}$-module. The degree at a point p $\deg_p(\mathcal{F})$ of $\mathcal{F}$ is the rank of ${\mathcal{F}_p}\!\diagup_{m_p\mathcal{F}_p}$ as a k_p-module.

The degree behaves similarly to the ordinary topological degree:

Proposition 1.5.13. *The degree satisfies the following conditions:*

1. *for all $p \in X$, $\deg_p(\mathcal{F}) \geq \deg(\mathcal{F})$.*
2. *The subset of X $\{p \in X \mid \deg_p(\mathcal{F}) \leq r\}$ is open for all r.*
3. *The degree is constant (and thus everywhere equal to $\deg(\mathcal{F})$) if and only if $\mathcal{F}$ is locally free.*

Proof. We'll give a sketch of the proof. We may suppose $X = \mathrm{spec}(A)$, so that $\mathcal{F} = \tilde{M}$, with $M = {A^r}\!\diagup_I$. Then, given prime ideal $p \in \mathrm{spec}(A)$, the dimension of ${\mathcal{F}_p}\!\diagup_{m_p\mathcal{F}_p}$ is $r - \dim_{k_p}({I_p}\!\diagup_{pI_p})$. This immediately implies the first point as the second term is zero at the generic point of X. To show the second point, we write a set of generators of I as a linear combination (with coefficients in A) of the generators of M, and consider the matrix of their coefficients. Then asking for the dimension of ${I_p}\!\diagup_{pI_p}$ to be lower than a given integer s is tantamount to asking for all minors of rank s of the coefficient matrix to have determinant 0 at p, which is a closed condition.

To show the third condition, choose $p \in X$. Let ${}^{\mathcal{F}_p}\!/_{m_p\mathcal{F}_p}$ be generated by $\alpha_1, \ldots, \alpha_d$. Then we can restrict to an affine open neighbourhood U of p such that $\alpha_1, \ldots, \alpha_d$ generate ${}^{\mathcal{F}_q}\!/_{m_q\mathcal{F}_q}$ for all $q \in U$. Then by Nakayama's Lemma we can conclude that $\mathcal{F}(U)$ is generated by d elements, and thus, as its degree is d at all points, must be free. □

We are ready to define the *degree of a finite morphism*:

Definition 1.5.16. Let $f : X \to Y$ a finite morphism of integral schemes. The *degree* of f $\deg(f)$ is the degree of the field extension $K(X)/K(Y)$. The degree at a point $p \in Y$ $\deg_p(f)$ of f is the dimension of $\mathcal{O}_{X_p}(X_p)$ as a k_p vector space, where X_p is the fiber of f at p.

While this seems quite distant from the previous definition, it is actually the same, as $f_*\mathcal{O}_X$ is a Quasi-coherent sheaf on Y.

Proposition 1.5.14. *If $f : X \to Y$ is a finite morphism and $\mathcal{F}$ a Quasi-coherent sheaf on X. Then $f_*\mathcal{F}$ is Quasi-coherent.*

Proof. Let $U = \operatorname{spec}(A)$ be an affine open subset of Y. Then $f^{-1}(U) = \operatorname{spec}(B)$ is affine, and B is a finite A-module. □

Proposition 1.5.15. *Let $f : X \to Y$ be a finite morphism of integral schemes. The following properties are true:*

1. *For all $p \in Y$, $\deg(f) \leq \deg_p(f)$.*
2. *The subset of Y $\{p \in Y \mid \deg_p(f) \leq r\}$ is open for all r.*
3. *The degree is constant (and thus everywhere equal to $\deg(f)$) if and only if f is flat.*

Proof. It suffices to notice that the degree of f at a point p (including the generic point) is equal to the degree of $f_*\mathcal{O}_X$ at p, and Apply Proposition (1.5.13). □

1.6 Divisors and curves

In this section, we'll develop some instruments of curve theory, leading to what is maybe the most important result in the study of curves: the *Riemann-Roch Theorem*. At first, let us assume X is a normal noetherian scheme of dimension 1. We'll develop the concept of *divisor*, which, as for riemaniann surfaces, is an important instrument for the study of curves.

Definition 1.6.1. Let X be a noetherian normal scheme of dimension 1. The *divisors group* of X $\mathrm{Div}(X)$ is the free abelian group on the set of closed points of X. A *divisor* D is an element of $\mathrm{Div}(X)$.

Consider now a *rational section* $\phi \in \mathcal{O}_{X,\xi}$. Using the theory of Dedekind domains we developed previously, we can naturally assign a divisor, which we'll name $\mathrm{div}(\phi)$ or simply (ϕ), to f.

Definition 1.6.2. Let $\phi \in \mathcal{O}_{X,\xi} \doteq K(X)$. Given a closed point $p \in X$, the local ring $\mathcal{O}_{X,p}$ is a DVR, and ϕ is naturally an element of $\mathrm{Frac}(\mathcal{O}_{X,p})$. The sum $\sum_{p\in X} \mathrm{v}_p(\phi)$ is a divisor, which we'll call the *divisor of* ϕ. If a divisor can be obtained this way we call it a *principal divisor*.

This is clearly well defined, but we should check the fact that the sum is finite: this is clear as given an affine open subset $U = \mathrm{spec}(A)$ there are only a finite number of prime ideals of A such that the valuation of ϕ is not zero by the theory of dedekind domains, and the complementary of U is finite.

Proposition 1.6.1. *The set of principal divisors is a subgroup of* $\mathrm{Div}(X)$*, which we'll call* $\mathrm{P}(X)$*.*

Proof. By the properties of valuations, $\mathrm{div}(\phi\psi) = \mathrm{div}(\phi) + \mathrm{div}(\psi)$, $\mathrm{div}(\frac{1}{\phi}) = -\mathrm{div}(\phi)$, $0 = \mathrm{div}(1)$. □

We are ready to define the *divisor class group* of X:

Definition 1.6.3. The *divisor class group* of X is $\mathrm{Cl}(X) \doteq {}^{\mathrm{Div}(X)}\!/_{\mathrm{P}(X)}$.

Actually, we could have done the whole construction of $\mathrm{Cl}(X)$ just assuming X to be a noetherian scheme regular in codimension 1, and using the set of points of codimension 1 rather than that of closed points.

Generally, there is a morphism $\mathrm{Pic}(X) \to \mathrm{Cl}(X)$. As we'll see, in our case this is an isomorphism.

Proposition 1.6.2. *There is a group morphsim* $\mathrm{Pic}(X) \to \mathrm{Cl}(X)$*.*

Proof. Let $\mathcal{F}$ be an invertible sheaf on X. Then $\mathcal{F}_\xi$ is a 1-dimensional vector space on $K(X)$. Given $p \in X$ let $s \in \mathcal{F}_\xi \setminus 0$, and let U be an affine open neighbourhood of p such that $\mathcal{F}_{|U} \simeq \mathcal{O}_U$. Name λ the isomorphism. We can extend λ uniquey so that $\mathcal{F}_\xi \simeq \mathcal{O}_{U,\xi}$. Let $s_p \in \mathcal{F}_\xi$ be the inverse image of 1. We define $\mathrm{v}_p(s) = \mathrm{v}_p(\frac{\lambda(s)}{\lambda(s_p)})$. As we've seen before, this construction does not depend on λ.
This way we have defined a divisor $\mathrm{div}(s)$. Let now s' be another nonzero element of $\mathcal{F}_\xi$. As $\mathcal{F}_\xi$ is a vector space of dimension 1 on $K(X)$, there is $\phi \in K(X)$ such that $s' = s\phi$, and we can easily check that $\mathrm{div}(s') = \mathrm{div}(s) + \mathrm{div}(\phi)$. Then the image of $\mathcal{F}_\xi$ in the class group of X is a single element, which we name the *divisor of* $\mathcal{F}$.
To see this is a group homomorphism, we just need to notice that if U is such that $\mathcal{F}_{|U} \simeq \mathcal{O}_U$, $\mathcal{G}_{|U} \simeq \mathcal{O}_U$ with isomorphisms λ_1, λ_2, the morphism $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}(U) \to \mathcal{O}_X(U)$ is induced by $s_1 \otimes s_2 \to \lambda_1(s_1)\lambda_2(s_2)$. □

In our case (X is a Dedekind scheme) this is an isomorphism:

Theorem 1.6.3. $\mathrm{Pic}(X) \to \mathrm{Cl}(X)$ *is injective.*

Proof. Suppose $\mathrm{Div}(\mathcal{F}) = 0$ in the class group. Let s be the section we chose to obtain our divisor. Then the divisor of s is equal to the divisor of ϕ for some rational section ϕ, and the divisor of $\phi^{-1}s$ is zero. We want to show that $\mathcal{F} = s\mathcal{O}_X$. As $\mathcal{F}$ is invertible, we just need to show it for an affine covering $\{U_i\}_{i\in I}$ such that $\mathcal{F}_{|U_i}$ is isomorphic to $\mathcal{O}_{U_i}$. We name λ_i the isomorphim relative to U_i. Then $\lambda_i(s)$ is an element of $\mathrm{Frac}(\mathcal{O}_X(U_i))$ such that its valuation at all nonzero primes is zero. As $\mathcal{O}_X(U_i)$ is a Dedekind domain, $\lambda_i(s)$ is invertible and thus s generates $\mathcal{F}_{|U_i}$ as a sheaf of $\mathcal{O}_{U_i}$-modules. □

To obtain this in a more general context, it would be sufficient to have X normal, so that for an affine open subset $U = \mathrm{spec}(A)$ we would have $A = \cap_{\mathrm{ht}(P)=1} A_P$ and we could reason exactly the same way as we just did. To show surjectivity, given a divisor D we'll exhibit an invertible sheaf whose divisor is equivalent to D in the class group.

Definition 1.6.4. Let X be noehterian normal scheme of dimension 1. Let $D = \sum_{p\in X_0} n_p p$ be a divisor. We name $\mathcal{O}_X(D)$ the sheaf of $\mathcal{O}_X$-modules defined by $\mathcal{O}_X(D)(U) = \{\phi \in K(X)^* \mid \mathrm{v}_p(\phi) + n_p \geq 0 \quad \forall p \in X_0 \cap U\} \cup 0$.

So $\mathcal{O}_X(D)$ is basically the sheaf of rational functions satisfying the conditions imposed by D, which we may think of as having zeros of order at least $|n_p|$ whenever $n_p \leq 0$ and having poles of order at most $|n_p|$ whenever $n_p > 0$.

Proposition 1.6.4. *$\mathcal{O}_X(D)$ is an invertible sheaf. The divisor of $\mathcal{O}_X(D)$ is D. If $D - D'$ is the divisor of a rational function, $\mathcal{O}_X(D)$ is isomorphic to $\mathcal{O}_X(D')$.*

Proof. Let p be a point of X. As $\mathcal{O}_{X,p}$ is a DVR, we can choose an affine neighbourhood $U = \operatorname{spec}(A)$ of p such that:

- p is the only point of U such that $n_p \neq 0$.
- p is a principal ideal of A.

Then if t_p is a generator for p, $\mathcal{O}_X(D)_{|U} = t_p^{-n_p}\mathcal{O}_U$. This also implies, by the construction of $\operatorname{div}(\mathcal{F})$ we described before, that the coefficient of p in $\operatorname{div}(\mathcal{O}_X(D))$ is n_p, as we can choose $1 \in \mathcal{O}_X(D)_\xi$ as our rational section s and $\phi \to {t_p}^{n_p}$ as a local isomorphism at p.
To prove the last assertion, if $D - D'$ is the divisor of a rational function ϕ, it is immediate that $\mathcal{O}_X(D') = \phi\mathcal{O}_X(D)$. □

More generally, it would have been sufficient to assume X noetherian and locally factorial to obtain the same result.

Corollary 1.6.5. *The morphism* $\operatorname{div} : \operatorname{Pic}(X) \to \operatorname{Cl}(X)$ *is an isomorphism, and* $\mathcal{F} \simeq \mathcal{O}_X(\operatorname{div}(\mathcal{F}))$.

Proof. We have shown div is both injective and surjective. Then an invertible sheaf is determined by its divisor, which implies the second assertion. □

So, given fitting hypoteses, the sheaves $\mathcal{O}_X(D)$ are a set of representatives of the isomorphism classes of invertible sheaves on X. A first step on the study of these sheaves is finding out whether $\mathcal{O}_X(D)$ has any global section or not.

Definition 1.6.5. A divisor is called *positive* if all its coefficients are equal to or greater than zero. An equivalence class of divisor is called *effective* if it is equivalent to a positive divisor.

Proposition 1.6.6. $\mathcal{O}_X(D)$ *has nonzero global sections if and only if* D *is effective.*

Proof. If ϕ is a global section of $\mathcal{O}_X(D)$, as ϕ is a rational function, the divisor $D + \operatorname{div}(\phi)$ is positive and equivalent to D. Conversely, if $D + \operatorname{div}(\phi)$ is positive, $\phi \in \mathcal{O}_X(D)$. □

We'll see much deeper results on the global sections of $\mathcal{O}_X(D)$ after restricting the scope of schemes we're considering to a very peculiar, yet immensely important subcategory, that of *curves*.

Definition 1.6.6. A *curve* over k is a projective k-scheme of dimension 1 such that $X \otimes_{\operatorname{spec} k} \operatorname{spec}(\overline{k})$ is irreducible and regular (these two properties are also called *geometric irreducibility* and *smoothness*).

An *affine curve* is an affine open subset of a curve. Notice that any geometrically irreducible and smooth affine algebraic variety of dimension 1 has an open immersion into its (normal) projective completion, and thus is an affine curve.

The regularity condition can be simplified if k is perfect:

Proposition 1.6.7. *If k is perfect, $X \times_{\operatorname{spec} k} \operatorname{spec}(\overline{k})$ is regular if and only if X is regular.*

Proof. See [3]. □

Corollary 1.6.8. *If k is perfect, and X has dimension 1, $X \times_{\operatorname{spec} k} \operatorname{spec}(\overline{k})$ is regular if and only if X is normal.*

Proof. This is clear as a curve is normal if and only if it is regular. □

Now, recall the normalization af an algebraic variety is finite; as finite morphisms are projective, the normalization of a projective variety is a projective variety. This implies that given a geometrically irreducible projective variety over a perfect field k, its normalization is a curve over k.

Curves are *Dedekind schemes*, schemes whose affine open subsets are isomorphic to the spectrum of a Dedekind domain. Now, consider a morphism of curves $f : X \to Y$. first, we state an important theorem due to CHevalley:

Theorem 1.6.9 (Chevalley)**.** *A proper, quasi-finite morphism of locally noetherian schemes is finite.*

Proof. See [3]. □

Proposition 1.6.10. *Let $f : X \to Y$ be a morphsim of curves over k. There are two cases:*

1. *f is constant.*
2. *f is surjective, flat, finite.*

Proof. As the structural morphism π of Y is separated, and the composition $f \circ \pi$ is the structural morphism of X, thus projective, f is projective too. Then $f(X)$ is a closed, connected subset of Y, implying it is either a point or Y. Now, recall a module over a Dedekind domain is flat if and only if it is torsion free. This implies a morphism from an integral scheme to a Dedekind scheme is flat if and only if it is dominant, so whenever f is not constant f is flat. Finally, f is finite because of Chevalley's theorem, as a morphism of finite type with finite fiber is always quasi-finite. □

For curves, checking wheter a morphism is an isomorphism is quite simple:

Proposition 1.6.11. *Let f be a noncostant morphism of curves. Then f is an isomorphism if and only if* $\deg(f) = 1$.

Proof. If f is an isomorphism it is clear that $\deg(f) = 1$. Now, suppose $f : X \to Y$ has degree 1. Let U be an affine open subset of Y, $V = f^{-1}(U)$. Then $\mathcal{O}_X(V)$ is a locally free $\mathcal{O}_Y(U)$-module, and thus there is an affine open subset U' of U such that $\mathcal{O}_X(f^{-1}(U'))$ is free of degree 1 over $\mathcal{O}_Y(U')$. Then $\mathcal{O}_X(f^{-1}(U'))$ is isomorphic to $\mathcal{O}_Y(U')$, and f is birational. Being finite and birational, by Proposition (1.4.6) f is a normalization morphism. As Y is normal and the normalization is unique up to isomorphism, f is an isomorphism. □

As f is finite, it defines a morphism $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$:

Definition 1.6.7. Let $f : X \to Y$ be a nonconstant morphism of curves over k. Given $p \in X$, $q = f(p)$, and a generator t_q of $\mathcal{O}_{Y,q}$ let $e_p(f) = \mathrm{v}_p(f^\sharp(t_q))$ be the *index of f at p*. We define $f^*(q) = \sum_{p \in f^{-1}(q)} e_p(f)p$. This extends linearly to an homomorphism $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$.

Definition 1.6.8. Let X be a curve over k, and let $D = \sum_{p \in X} n_p p \in \mathrm{Div}(X)$ be a divisor. We define the *degree of D* as $\sum_{p \in X} n_p \, [k(p) : k]$. The degree is a morphsim $\mathrm{Div}(X) \to \mathbb{Z}$.

The degree does not really depends on the base field k.

Proposition 1.6.12. *Let X be a curve, let k'/k be an algebraic separated extension of fields, and let $\pi : X \times_{\mathrm{spec}\, k} \mathrm{spec}(k') \to X$ be the canonical projection. Then the degree of $\pi^{-1}(D)$ is equal to* $\deg(D)$.

Proof. See [3]. □

Pulling back divisors interacts well with the degree:

Proposition 1.6.13. *Let f be a morphism of curves over k. The degree of $f^*(D)$ is* $\deg(f)\deg(D)$.

Proof. It suffices to show it for a point $q \in Y$. As f is flat, $\deg(f) = \deg_q(f)$. We have:

$$\begin{aligned} \deg(f) = \dim_{k(q)}(X_q) = \dim_{k(q)} \textstyle\prod_{p \in f^{-1}(q)} {\mathcal{O}_{X,p}}\!\diagup_{f^\sharp(t_q)\mathcal{O}_{X,p}} \\ = \textstyle\sum_{p \in f^{-1}(q)} \dim_{k(q)} {\mathcal{O}_{X,p}}\!\diagup_{(t_p)^{e_p(f)}\mathcal{O}_{X,p}} = \sum_{p \in f^{-1}(q)} e_p(f)\,[k(p) : k(q)] \\ = \textstyle\sum_{p \in f^{-1}(q)} \frac{e_p f [k(p):k]}{[k(q):k]} = \frac{\deg(f^*(q))}{\deg(q)}. \end{aligned}$$

□

We would like to extend degree to the class group of X; to do this we must first show the group of principal divisor is contained in the kernel of $\deg : \mathrm{Div}(X) \to \mathbb{Z}$. We will show this in two steps:

Proposition 1.6.14. *Let $f \in K(X)$. then $f \in \mathcal{O}_X(U)$ for some open subset U, and f defines a morphsim $\tilde{f} : U \to \mathbb{A}^1{}_k$ by the morphism of k-algebras $x \to f$. This can be extended to a morphism $\tilde{f} : X \to \mathbb{P}^1{}_k$.*

Proof. As $X \setminus U$ is a finite set of closed points, it suffices to show we can extend $\tilde{f}$ to $U \cup p$ for any $p \in U^c$. First, notice $U \cup p$ is open. If $\mathrm{v}_p(f) \geq 0$ by Proposition (1.1.5) f belongs to $\mathcal{O}_X(V)$ for any affine open subset V of U, and thus it belongs to $\mathcal{O}_X(V)$ by glueing, so we have no problem extending the morphism. If $\mathrm{v}_p(f) < 0$ then f^{-1} belongs to $\mathcal{O}_{X,p}$. We can choose an open neighbourhood V of p such that:

- $V \cap U = V \setminus p$.
- $\mathrm{v}_q(f) \leq 0$ for all q in V.

then we can define a morphism $V \to \mathbb{A}^1{}_k$ by $y \to f^{-1}$. Now, by identifying this copy of $\mathbb{A}^1{}_k$ with the open subset $\mathrm{proj}(k\,[x,y])_{(x)}$ of $\mathrm{proj}(k\,[x,y]) = \mathbb{P}^1{}_k$, and the one we used before with the open subset $\mathrm{proj}(k\,[x,y])_{(y)}$ we obtain a morphism $U \cup p \to \mathbb{P}^1{}_k$ by glueing. As one would expect, this morphsim sends p to the point at infinity. □

Corollary 1.6.15. *The divisor of a rational function has degree zero.*

Proof. It's immediate that $\mathrm{Div}(f) = f^*(0) - f^*(\infty)$. Then $\deg(\mathrm{div}(f)) = \deg(f^*(0)) - \deg(f^*(\infty)) = \deg(f) - \deg(f) = 0$. □

Corollary 1.6.16. *The degree of a class of divisors is well defined.*

Lastly, we would like for the pullback of a principal divisor to be principal.

Proposition 1.6.17. *Let $f : X \to Y$ be a nonconstant morphism of curves. Then the pullback of a principal divisor is principal. This implies f^* induces a morphism $f^* : \mathrm{Cl}(Y) \to \mathrm{Cl}(X)$.*

Proof. f induces a morphsim $f^\sharp : K(Y) \to K(X)$. It's easy to verify that $f^*(\mathrm{div}(\psi)) = \mathrm{div}(f^\sharp(\psi))$. □

We have almost all we need to state the *Riemann-Roch Theorem*. We need a few more definitions, whose theory we won't develop for the sake of brevity.

Definition 1.6.9. Let X be a scheme, F a sheaf of $\mathcal{O}_X$ modules. $\mathrm{H}^i(X, \mathcal{F})$ is the *i-th Čech Cohomology group* of $\mathcal{F}$.

This is defined the same way as any Čech Cohomology; as Čech Cohomology is omnipresent in Mathematics, we'll suppose the reader has at least an idea of how it is defined. There are a few properties peculiar to schemes which it's interesting to state:

Proposition 1.6.18. *Let X be a noetherian scheme, $\mathcal{F}$ a coherent sheaf on X. Then:*

- $\mathrm{H}^0(X, \mathcal{F}) = \mathcal{F}(X)$ *(this is always true).*
- *If X is affine,* $\mathrm{H}^i(X, \mathcal{F}) = 0$ *for all* $i \geq 1$.
- $\mathrm{H}^i(X, \mathcal{F}) = 0$ *for all i greater than the dimension of X.*
- *If X is a proper* $\mathrm{spec}(A)$*-scheme,* $\mathrm{H}^i(X, \mathcal{F})$ *is a finite A-module for all i.*

Given a morphism of schemes $f : X \to Y$, there is a canonical sheaf of $\mathcal{O}_X$-modules associated to it. It is the sheaf of *Kähler Differentials* $\Omega_{X/Y}$. If X is an Y-scheme and the morphism f is the structural morphism of X we'll omit Y and just use the symbol Ω_X.

Proposition 1.6.19. *Let X be a geometrically irreducible, smooth variety. Then Ω_X is locally free of rank equal to the dimension of X.*

Proof. See [3]. □

In the case of curves, this implies Ω_X is an invertible sheaf.
Khaler Differentials and Čech Cohomology are deeply tied, as we're about to see. The theorem we are going to enounce is actually a corollary of a much stronger one, the *Serre's Duality Theorem*.

Theorem 1.6.20 (Serre)**.** *Let X be a proper, geometrically connected, smooth scheme over k of dimension* 1*. Let $\mathcal{F}$ be an invertible sheaf on X. Then:*

1. $\mathrm{H}^1(X, \Omega_X) \simeq k$.
2. *There are nondegenerate bilinear pairings:*

$$\mathrm{H}^0(X, \mathcal{F}) \otimes_k \mathrm{H}^1(X, \mathcal{F}^{\mathrm{v}} \otimes_{\mathcal{O}_X} \Omega_X) \to k$$
$$\mathrm{H}^1(X, \mathcal{F}) \otimes_k \mathrm{H}^0(X, \mathcal{F}^{\mathrm{v}} \otimes_{\mathcal{O}_X} \Omega_X) \to k$$

3. $\mathrm{H}^1(X, \mathcal{F}) \simeq \mathrm{H}^0(X, \mathcal{F}^{\mathrm{V}} \otimes_{\mathcal{O}_X} \Omega_X)^{\mathrm{v}}$,$\mathrm{H}^0(X, \mathcal{F}) \simeq \mathrm{H}^1(X, \mathcal{F}^{\mathrm{v}} \otimes_{\mathcal{O}_X} \Omega_X)^{\mathrm{v}}$.

Proof. See [3] for an extremely general treatment of the subject. □

Definition 1.6.10. Let X be a curve over k. The *genus* of X is $\dim(\mathrm{H}^1(X, \mathcal{O}_X))$. The genus of a projective, geometrically connected algebraic variety of dimension 1 is that of its normalization. The genus of an affine algebraic variety of dimension one X is that of any projective completion $X \to \tilde{X}$.

The genus is an important numerical invariant of a curve. If k is a subfield of $\mathbb{C}$, it is the usual topological (and differential) genus. Before we finally enounce the *Riemann Roch-Theorem*, notice that the dual sheaf of $\mathcal{O}_X(D)$ is $\mathcal{O}_X(-D)$. This should at least give a hint on the deep ties of the *Riemann Roch-Theorem* with the duality theorem we just enounced.

Theorem 1.6.21 (Riemann-Roch)**.** *Let X be a curve of genus g over a field k. Then:*

$$\dim_k(\mathrm{H}^0(X, \mathcal{O}_X(D))) = \deg(D) + 1 - g(X) + \dim_k(\mathrm{H}^0(X, \mathcal{O}(-D) \otimes_{\mathcal{O}_X} \Omega_X).$$

Proof. See [3]. □

Chapter 2

Siegel's Theorem

In this chapter we are going to prove the famous *Siegel's Theorem* on S-integral points, following a proof by Professor Umberto Zannier (from [8]). The crucial point of the proof will be the introduction of the v-adic Topology on algebraic varieties, which we'll discuss soon after introducing the notion of Quasi-S integral sets and the theorem itself.

2.1 Quasi-S integral sets

Quasi-S integral sets are a slight generalization on the concept of S-integral points, which are just rational points whose coordinates are integers except for a finite number of prime factors; actually, given a Quasi-S integral set, there is always a linear trasformation sending it to a set of S-integral points, as we'll see. Quasi-S integral sets are however a much better object to study since they are defined independently of coordinates and behave well under morphisms of affine varieties.

Definition 2.1.1. Let k be a field, $S \subseteq M_k$ a finite set of absolute values containing all the archimedean ones. We name K_S the subring of k defined by $K_S = \{\alpha \in k \mid |\alpha|_v \leq 1 \forall v \in M_k \setminus S\}$. Being a localization of $\mathcal{O}_k$, K_S is a Dedekind domain.

To get a clearer idea of K_S, suppose $\mathcal{O}_k$ is an UFD. Let γ_v be a generator for the prime ideal relative to $v \in S$. Then K_S is the subring of $k = \mathrm{Frac}(\mathcal{O}_k)$ of all fractions $\frac{a}{b}$, where $a \in \mathcal{O}_k$ and b is a product of the γ_v.

Definition 2.1.2. Let X be an affine algebraic variety over a field k, and let S be a proper set of absolute values over k. A set of k-rational points Σ is Quasi-S integral if and only if for any element $f \in \mathcal{O}_X(X)$ there is $a_f \in k^*$

such that for all $p \in \Sigma$ the residue class of f modulo the maximal ideal m_p is an S-integer.

There are three facts to observe at once: first, this notion is meaningless for finite sets, as every such set is Quasi-S integral, second, we can always choose $a_f \in K_S$, and third, it is sufficent to check this condition for a set of generators of $\mathcal{O}_X(X)$. We can also describe Quasi-S integrality by means of the fibered product:

Proposition 2.1.1. *Let X be an algebraic variety over k, and Σ a set of k-rational points of X. The following properties are equivalent:*

1. *The set Σ is Quasi-S integral*
2. *There is an K_S-scheme of finite type $\boldsymbol{X}$ such that $X = \boldsymbol{X} \times_{\mathrm{spec}(K_S)} \mathrm{spec}(k)$, and every point x of Σ extends to a K_S valued point of $\boldsymbol{X}$*
3. *There is an affine K_S scheme of finite tipe satisfying the previous property.*

Proof. to prove 1) $\Rightarrow$ 3), let us choose an immersion $X \to {\mathbb{A}_k}^N$. We can then multiply the coordinates $x_1, \ldots, x_N$ by $a_{x_1}, \ldots, a_{x_N}$ so that the points in Σ are now K_S valued, then take the K_S-subalgebra A generated by these. It is now clear that $spec(A) \times_{\mathrm{spec}(K_S)} \mathrm{spec}(k) = X$, and the points of Σ extend to K_S-valued points of $spec(A)$ by construction. Clearly 3) $\Rightarrow$ 2), so we just need to verify that 2) $\Rightarrow$ 1). To see that, we choose $f \in \mathcal{O}_X$; there is $a_f \in K_S \setminus \{0\}$ such that $a_f f$ extends to an element g of $\mathcal{O}(\mathbf{X})$, then, as the points of Σ extend to K_S valued points of $\mathbf{X}$, the residue class of $a_f f = g \otimes 1$ at a point of Σ is the same as the class at its extension: as the extensions $p \in \Sigma$ are K_S valued points, we have $a_f f(p) \in K_S$. □

In the proof of 1) $\Rightarrow$ 3) we can also observe that by a simple choice of coordinates any Quasi-S integral set becomes a set of K_S valued points. We are now intrested in seeing how Quasi-S integral sets behave under morphisms of affine varieties over k.

Proposition 2.1.2. *1. If $\phi : X \to Y$ is a morphism of affine varieties over k, the image of a Quasi-S integral set of X is a Quasi-S integral set of Y.*

2. If $\psi : X \to Y$ is a finite morphism of affine varieties over k and Σ is a set of k-rational points of X, the image of Σ is Quasi-S integral if and only if Σ is Quasi-S integral.

Proof. 1. This is clear as the residue class at a point p of $f \in \mathcal{O}_Y(Y)$ is the same as the class at any of the counterimages of p.

2. One implication has already been proven. To check the other one, suppose Σ is a Quasi-S Integral set of Y. If ψ is finite, we have that $\mathcal{O}_X(X)$ is integral over $\mathcal{O}_Y(Y)$. Let f be an element of $\mathcal{O}_X(X)$, then f satiesfies a monic polynomial relation over the image of $\mathcal{O}_Y(Y)$. Let this realtion be $f^m + g_1 f^{m-1} + \ldots + g_m = 0$. We can take the product $\Delta = a_{g_1} \ldots a_{g_m}$, so that $\Delta g_i(p) \in K_S$ for all i, and consider the relation $(\Delta f)^m + \Delta g_1 (\Delta f)^{m-1} + \ldots + \Delta^m g_m = 0$ obtained by multiplying the previous one by Δ^m. For each $p \in \Sigma$, by valuating the relation at p, we obtain a monic polynomial relation for $\Delta f(p)$ with coefficents in K_S. As K_S is integrally closed, we can conclude that $\Delta f(p) \in K_S$, as we wanted.

□

The second assertion, while being a step in the right direction, is still unsatisfactory, as it gives informations only on points of Y which can be lifted to X over k. If we take the hypothesis that ψ is not only finite, but can be extended to an etalé covering beetween the projective completions of X and Y, we can get a much better result by using two famous theorems, the *Chevalley-Weil Theorem* and *Hermite's Theorem.*
First, we'll need some definitons:

Definition 2.1.3. Let $f : X \to Y$ be a morphism of finite type. Suppose Y is locally noetherian.

- We say f is *smooth* if f is flat and the fiber X_y is smooth for every point $y \in Y$.
- We say f is *Étale* if f is smooth and the fiber X_y has dimension zero for every point $y \in Y$.

Theorem 2.1.3 (Chevalley-Weil)**.** *Let $f : X \to Y$ be a covering (i.e. an etalé surjective morphism) of projective varieties over a field k with a proper set of discrete values M_k. Then there is $d \in \mathcal{O}_k$ such that for every point y of $Y(K)$, where K is a finite extension of k, the discriminant of the field extension $k(f^{-1}(y))/k(y)$ divides d.*

Proof. See [5]. □

This substantially means that the extensions $k(f^{-1}(y))/k(y)$ are unramified outside the prime ideals corresponding to the prime factors of $\langle d \rangle$.

Theorem 2.1.4 (Hermite)**.** *There are only a finite number of fields of given degree and unramified outside a fixed finite set of absolute values over k.*

Now, if we have a covering of projective varieties, the degree $[k(f^{-1}(y)) : k(y)]$ is bounded by the degree of the morphism, and combining the two theorems just stated, we obtain:

Lemma 2.1.5. *Let $f : X \to Y$ be an étale surjective morphism of projective varieties over a field k with a proper set of discrete values M_k, then for all finite extensions k' of k, we have $f^{-1}(Y(k')) \subset X(k'')$, where k'' is a finite extension of k.*

Proof. As all the extensions have bounded degree and are unramified outside a finite set of absolute values, they are all contained in a finite number of finite extensions of k. We can then take the composed field of all these extensions, which is still a finite extension of k. □

Now, let X be an algebraic variety over k, and $S \subseteq M_k$ a proper set of absolute values over k. For all finite extetions k' of k, let $S_{k'}$ be the (proper) subset of $M_{k'}$ all the absolute values of k' extending the values of S. We name $F_S(X, k')$ the assertion "if Σ is a set of Quasi-$S_{k'}$ integral points of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k')$, Σ is finite". We name $F_S(X)$ the assertion " $F_S(X, k')$ is true for all finite extensions k' of k ". With this terminology, we can now state:

Proposition 2.1.6. *1. If k' is a finite extension of k, $F_S(X, k') \Rightarrow F_S(X, k)$.*

2. *If $\phi : X \to Y$ is a morphism of affine varieties over k with finite fibers, $F_S(Y, k) \Rightarrow F_S(X, k)$.*

3. *If $\phi : X \to Y$ extends to a covering $\tilde{X} \to \tilde{Y}$, where $\tilde{X}, \tilde{Y}$ are their projective closures, we have $F_S(X) \Leftrightarrow F_S(Y)$.*

4. *If X has dimension 1 and $X^\nu \to X$ is a normalization, $F_S(X^\nu) \Rightarrow F_S(X)$.*

Proof. 1. Let us choose a set of generators $\{f_1, \ldots, f_r\}$ of $\mathcal{O}_X(X)$, and let $\{g_1, \ldots, g_r\}$ be their images trought ${\pi_1}^\sharp$. $\{g_1, \ldots, g_r\}$ is then a set of generators for $\mathcal{O}(X \times_{\mathrm{spec}(k)} \mathrm{spec}(k'))$. As the first projection is a morphism over k, the residue class of f_i at a rational point p of X is the same as the class of g_i at its inverse image (the map is $1:1$ restricted to the set of k-rational points of X), which implies there are $a_1, \ldots, a_r$ such that $\{a_1 g_1(p), \ldots, a_r g_r(p)\} \subset K_S \subset K'_{S'}$. As we only need to check Quasi-S integrality on a set of generators, we have that for all sets Σ Quasi-S integral on X, Σ is Quasi-S' integral on $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k')$. This implies our thesis.

2. Let Σ be a Quasi-S integral set of X, then by Proposition (2.1.2) its image is a Quasi-S integral set of Y, thus it is finite. As ϕ has finite fibers, Σ must be finite itself. If ϕ is a normalization, Proposition (2.1.2), assertion (3) immidiately implies $F_S(X, k) \Rightarrow F_S(Y, k)$.

3. By applying (2) to $\phi \otimes_k \mathrm{Id} : X \times_{\mathrm{spec}(k)} \mathrm{spec}(k') \to Y \times_{\mathrm{spec}(k)} \mathrm{spec}(k')$ for all extensions k' we have $F_S(Y) \Rightarrow F_S(X)$. To show the other

implication, suppose we have $F_S(X)$ and let Σ be a Quasi-S integral set of Y. We have already shown that there is a finite extension k' such that the inverse image of Σ is made up of k'-rational points. We can now consider $\phi \otimes_k \mathrm{Id} : X \times_{\mathrm{spec}(k)} (k') \to Y \times_{\mathrm{spec}(k)} \mathrm{spec}(k')$. By (1) and (2.1.2) $\phi^{-1}({\pi_1}^{-1}\Sigma)$ is Quasi-S' integral, therefore finite. Then its image ${\pi_1}^{-1}\Sigma$ is finite, and as its points correspond $1:1$ to the points of Σ, Σ must be finite too. We have proven $F_S(X) \Rightarrow F_S(Y,k)$, and the same proof holds for any extension k' of k, so that we have $F_S(X) \Leftrightarrow F_S(Y)$.

4. As the normalization morphism is birational, finite and surjective (by the going-down theorem), if X has an infinite Quasi-S integral subset its inverse image contains infinitely many k-rational points, and we can use (2.1.2) to conclude.

□

Finally, we need to define the concept of "points at infinity":

Proposition 2.1.7. *Let X be a geometrically connected, irreducible affine algebraic variety over k of dimension one. There is a unique projective completion $i : X \hookrightarrow \tilde{X}$ such that $\tilde{X}$ is normal at the points of $\tilde{X} \setminus X$. The points of $\tilde{X} \setminus X$ are the* points at infinity *of X. If the divisor $\tilde{X} \setminus X$ has degree d, we'll say X has d points at infinity.*

Proof. Consider any projective closure $\overline{X}$ of X. Let U be an affine open subset of $\tilde{X}$ containing $\tilde{X} \setminus X$ and such that $U \cap X \subseteq X^{\mathrm{norm}}$. Let $\tilde{X}$ be any projective completion satisfying the property above. Then restricted to $U \cap X$ the inclusion i is an isomorphsim. By Theorem (1.4.3) the inverse of i can be extended to a morphism $j : \tilde{X}^{\mathrm{norm}} \to X$. This is finite and birational, thus a normalization. Then by construction $\tilde{X}$ is isomorphic to the glueing of X with the normalization of U. This shows $\tilde{X}$ is unique. Conversely, let U be as above. The normalization $U^v \to U$ is an isomorphism when restricted to X, and thus it glues to X via $V \cap U$. We obtain a scheme Y that is finite over $\overline{X}$, and thus projective, has an affine open subset V isomorphic to X and is normal at the points of $\tilde{X} \setminus V$, thus satisfyies the conditions above. □

We can now state *Siegel's Theorem*, and proceed to show how we can use the tools we just created to simplify the problem of proving it:

Theorem 2.1.8 (Siegel)**.** *Let k be a field, S be a proper and finite set of absolute values on k, and X an affine geometrically irreducible algebraic variety over k of dimension one. If X has an infinite set of Quasi-S integral points, it has genus* 0 *and at most two points at infinity (counted with multiplicity).*

The statement holds true if we substitute k with a finite extension k' and S with S'. We can then restate it as "Any irreducible affine curve X over k satisfies $F_S(X)$ unless it has genus 0 and at most two points at infinity". By Proposition (2.1.6) it is sufficient to check it for a finite extension k' of k, and for a normalization X^ν of X. Moreover, if X has genus one or more and less than three points at infinity, let us consider the *Étale fundamental group* of its projective completion $\tilde{X}$. We have:

Theorem 2.1.9. *Let $\tilde{X}$ be a curve over an algebraically closed subfield k of $\mathbb{C}$, and let $i : \tilde{X} \to \mathbb{P}^n{}_k$ be a closed immersion. Let G be the topological fundamental group of the set of closed points of $\tilde{X} \times_{\mathrm{spec}(k)} \mathrm{spec}(\mathbb{C})$, endowed with the topology induced by $i \otimes_k \mathrm{Id}_{\mathbb{C}} : \tilde{X} \times_{\mathrm{spec}(k)} \mathrm{spec}(\mathbb{C}) \to \mathbb{P}^n(\mathbb{C})$ by pulling back the usual differential topology of $\mathbb{P}^n(\mathbb{C})$. The* Étale Fundamental Group *of $\tilde{X}$ is isomorphic to the profinite completion $\hat{G}$ of G.*

Proof. For a full treatment of the subject, see [14]. □

As with the topological fundamental groups, finite quotients of the Étale fundamental group of a curve correspond to étale coverings of curves. Recall now the fundamental group of a Riemann surface depends only on its genus and for $g \geq 1$ it has arbitrarily large finite quotients. Since the "differential realization" of a curve is a Riemann surface, if $g(\tilde{X})$ is greater than or equal to 1 after base changing to a finite extension of our base field k we can choose a finite étale covering of curves $\pi : \tilde{Y} \to \tilde{X}$ of degree ≥ 3. Then, if Y is the inverse image of X, and thus an affine variety, Y has three or more points at infinity and $F_S(X) \Leftrightarrow F_S(Y)$.

Remark 2.1.10. *We have reduced the proof of Siegel's Theorem to proving the following statement: if X is an affine curve with at least three points at infinity (counted with multiplicity), there is a finite extension k' of k such that all Quasi-S' integral sets of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k')$ are finite.*

2.2 The v-adic topology

In this section, we ll'introduce a number of new topologies on an algebraic variety X, each corresponding to a topology on the base field k. This will prove fundamental for counting the integral points of X. First, let us define the v-adic topology on the vector space k^n:

Definition 2.2.1. Let k be a field, and v an absolute value over k. The v-adic topology on k is the topology defined by the norm induced by v. The v-adic topology on k^n is the only topology that makes it into a topological vector space with respect to the v-adic topology on k.

While this definition is quite abstract, we can construct the v-adic topology as a metric topology on k^n explicitly by combining that of k with one of the usual norms we have on vector spaces. All the metrics we obtain this way are topologically equivalent, i.e. they differ by a bounded function, thus giving rise to the same topology (the product topology).
With this definition only, it is still quite unclear what kind of topology we should define even for an affine variety X, as it gives us an idea only for the set of k-rational points of X, which can be very small unless k is algebraically closed, which is not the case. An idea is to define the v-adic topology on X by base changing to an algebraically closed field $\overline{k}$, extending v to $\overline{k}$ and taking the topology induced by the first projection:

Lemma 2.2.1. *Let p be a point of a topological space X, $\overline{p}$ its closure. Then for all open sets U of X, $p \in U$ if and only if $\overline{p} \cap U \neq \emptyset$.*

Proof. Suppose p does not belong to an open set U. Then $X \setminus U$ is a closed set containing p, so $\overline{p} \subseteq X \setminus U$. The other implication is trivial. □

This shows that if we already know the closure of all points of a topological space, we just need these sets to describe its topology. Now, let's recall this:

Remark 2.2.2. *The closed points of an algebraic variety are* everywhere dense*, which means any closed or open sets is determined by its intersection with the set of closed points. We'll call X_0 the set of closed points of X.*

Proof. This is a direct consequence of *Hilbert's Nullstellensatz*. □

When building the v-adic topology of an algebraic variety, we want to preserve the correspondence beetween points and irreducible closed sets of X. Then there is only one possible choice of topology:

Definition 2.2.2. Let X be an affine variety, $f_1, \ldots, f_r$ a set of generators for $\mathcal{O}_X(X)$, and $i : (X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}))_0 \to \overline{k}^r$ the inclusion $p \to$

$(f_1(p), \ldots, f_r(p))$. If we equip $\overline{k}^r$ with the $\overline{v}$-adic topology, where $\overline{v}$ is any extension of v, the map i defines a metric on $(X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}))_0$. This in turn defines a topology on $X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$ by choosing, for all $p \in X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}) \setminus (X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}))_0$, $\overline{p} = \mathrm{V}(\mathrm{I}(p))$. We define the v-adic topolgy of X as the topology induced by the projection π_1.

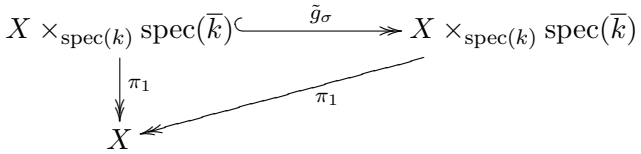
Remark 2.2.3. *The closure of a point $p \in X$ is the same for the v-adic topology and the Zariski topology, and any open or closed set V for the v-adic topology is determined by $V \cap X_0$.*

Proof. If $X = X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$, our definition implies the first property. If X is not defined over an algebraically closed field, it stems from the fact that $\pi^{-1}(\overline{p}) = \overline{\pi^{-1}(p)}$ for the Zariski topology. To check the second property it is sufficent to notice that the closure of p is determined by its closed points for all p in X. □

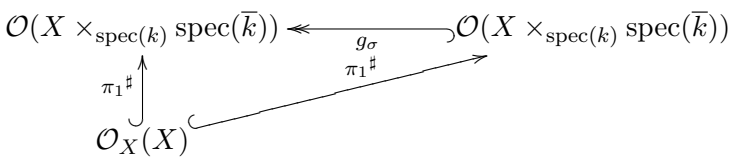
We have apparently made two arbitrary choices: we chose a set of generators for $\mathcal{O}_X(X)$ and an extension $\overline{v}$ of v. The first can be chosen in countably many way, while the second has more than countable choices! We need to show the topology we defined does not depend on these choices.

Proposition 2.2.4. *The v-adic topology on an affine variety X does not depend on the extension $\overline{v}$ we chose.*

Proof. Recall by Theorem (1.2.9) that given two extensions $\overline{v}, \overline{v}'$ of v there is a morphism σ in the Galois group of $\overline{k}$ over k such that $\overline{v} = \overline{v}' \circ \sigma$. Given such morphism $\sigma \in \mathrm{Gal}(\overline{k}/k)$, σ induces an automorphism of k-algebras $f_\sigma : \overline{k}[x_1, \ldots, x_r] \to \overline{k}[x_1, \ldots, x_r]$ which in turn induces a morphism $g_\sigma : \mathcal{O}(X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})) \cong \overline{k}[x_1, \ldots, x_r]/I \to \overline{k}[x_1, \ldots, x_r]/\sigma(I)$; as I is generated by elements in $k[x_1, \ldots, x_r]$, $\sigma(I) = I$, and g_σ is an automorphism of $\mathcal{O}(X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}))$, corresponding to an automorphism $\tilde{g}_\sigma$ of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$ which sends the v-adic topology of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$ to its v'-adic topology. We now consider the diagram:



And the corresponding morphisms of rings:



As g_σ is the identity restricted to the image of $\mathcal{O}_X(X)$, the second diagram commutes, which implies that the first one does too. Then the two projections $\pi_1, \pi_1 \circ \tilde{g}_\sigma$ are the same and therefore induce the same topology on X. As $\tilde{g}_\sigma$ maps the $\overline{v}$-adic topology on $X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$ to the $\overline{v}'$-adic topology, these two topologies induce the same topology on X. □

Proposition 2.2.5. *A morphism of affine varieties is continuous for the v-adic topology. In particular, an isomorphism of varieties is also a homeomorphism.*

Proof. First, we need to show that a morphism of affine varieties $X :\to Y$ sends X_0 to Y_0. We have this commutative diagram:

$$\begin{array}{ccc} X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}) & \xrightarrow{\phi \times \mathrm{Id}} & Y \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}) \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_1} \\ X & \xrightarrow{\phi} & Y \end{array}$$

Let us choose sets of generators $\{f_1, \ldots, f_r\}$ for $\mathcal{O}_X(X)$ and $\{g_1, \ldots, g_s\}$ for $\mathcal{O}_Y(Y)$. We can write $\phi^\sharp(g_i) = p_i(f_1, \ldots, f_r)$. This means the image of a rational point $(\lambda_1, \ldots, \lambda_r)$ is $(p_1(\lambda_1, \ldots, \lambda_r), \ldots, p_s(\lambda_1, \ldots, \lambda_r))$, which implies the induced morphism $f \otimes \mathrm{Id}$ sends closed points of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$ to closed points of $Y \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$. As the diagram commutes and the projections send closed points to closed points ($\mathrm{spec}(\overline{k})$ is a projective scheme), we can choose any closed inverse image of a closed point p of X and use the commutativity of the diagram above to conclude $f(p)$ is closed.
Now, the first projection π_1 is continuous by definition for the v-adic topology. By the diagram above it is then sufficent to check the continuity of $f \times \mathrm{Id}$. Let us recall that all rational maps $\overline{k}^r \to \overline{k}^s$ are continuous for the $\overline{v}$-adic topogy: it is then clear that the restriction $(X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k}))_0 \hookrightarrow \overline{k}^r$ is continuous, which implies our thesis. we can now observe that all choices of generators are equivalent, as changing generators is an isomorphism of affine varieties, which induces a bijective map continuous along with its inverse. □

Remark 2.2.6. *While an isomorphism fixes the v-adic topology, we cannot expect it to fix the metric on $X(k)$ too. Generally, the metric will change by a bounded function.*

Lemma 2.2.7. *1. Let X be an affine variety and U an affine open subset of X. Then the v-adic topology of U is homeomorphic to the subset topology.*

2. *Let X be an affine variety and V a closed subset of X. Then the v-adic topology of V (equipped with the structure of* $\operatorname{spec}(\mathcal{O}(X)/I(V))$*) is homeomorphic to the subset topology.*

Proof. 1. U is birational to its closure, which will be a finite union of irreducible components of X. As rational maps are contuinuous for the v-adic topology, the inclusion is an homeomorphism with the image.

2. If V is closed, the immersion $V \times_{\operatorname{spec}(k)} \operatorname{spec}(\overline{k}) \to \overline{k}$ is induced by the affine structure of V by choosing the same generators we chose for $\mathcal{O}_X(X)$, which by Proposition (2.2.5) is homeomorphic to the topology induced by its realization as $\operatorname{spec}(\mathcal{O}(X)/I(V))$.

□

We can now define the v-adic topology for any algebraic variety:

Proposition 2.2.8. *Let X be an algebraic variety over k and v an absolute value. Let $(U_i)_{i\in I}$ be a covering of affine open subsets. The v-adic topologies on these subset are compatible and the topology defined this way does not depend on the particular choice of affine covering.*

Proof. Let U, V be two affine open subsets of X. As X is separated, $U \cap V$ is affine. Then by the lemma just stated the topologies on $U \cap V$ induced by those on U and V are both homeomorphic to the v-adic topology on $U \cap V$. This shows that any two affine charts are compatible, proving our statement. □

Definition 2.2.3. We'll call the topology we just defined the v-adic topology of X.

Corollary 2.2.9. *Morphisms of algebraic varieties are continuous for the v-adic topology. Open and closed immersions are homeomorphisms onto the image.*

Proof. We can always choose a finite covering $\{U_i\}_{i\in I}$ such that for all i the restriction is an affine morphism. As the morphism is continuous on all U_i, it is globally continuous. We can check the second statement on an affine covering by using Lemma (2.2.7). □

We have defined a topology on X which, if restricted to rational points, is induced by a metric. Our next objective is finding some good compactness property. Clearly we cannot hope to find any non-trivial compact subset if our base field is not complete with respect to the metric induced by v, as any compact metric space is complete. We have then to consider the v-adic completion of k, which we'll name k_v.

Proposition 2.2.10. *Let k be a field, v an absolute value on k and V a finite k-module. The following conditions are equivalent:*

1. *Any bounded closed set of V is compact.*
2. *The unit sphere of X is precompact.*
3. *k, endowed with the v-adic topology, is locally compact (this implies k is complete with respect to v).*

Proof. (1) $\Rightarrow$ (2) is trivial; to show (2) $\Rightarrow$ (3), if (3) were false, The closure of the unit sphere of V would contain a finite product of non-compact closed sets of k, which is not compact. To show (3) $\Rightarrow$ (1), let U be a pre-compact open surrounding of 0. Its closure contains $B_\epsilon(0)$ for some ϵ and is contained in $B_M(0)$ for some M. Let T be a bounded closed set of V. Then we can multiply U by a constant α in k such that $T \subset \overline{U}^r$ where $r = \dim(V)$. Now T is a closed subset of a compact set, which implies it's closed. □

We can obviously define the v-adic topology in the exact same way for a variety over k_v. Clearly, this may well have too few properties in common with our usual topology to be of use. The following proposition shows this is not the case.

Proposition 2.2.11. *Let X be an algebraic variety over $k = \overline{k}$, v an absolute value on k, and $\tilde{v}$ an extension of v to k_v. The projection $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v) \to X$ induces an homeomorphism of X_0 onto its inverse image.*

Proof. We can reduce to the affine case. The projection is then induced by the inclusion $\mathcal{O}_X(X) \to \mathcal{O}_X(X) \otimes k_v$, and the inverse image of a closed point p consists of all the prime ideals of $\mathcal{O}_X(X) \otimes k_v$ containing the image of the corresponding maximal ideal m_p. We can now identify $\mathcal{O}_X(X) = k[x_1, \ldots, x_r]/I, \mathcal{O}_X(X) \otimes k_v = {k_v}[x_1, \ldots, x_r]/I \otimes k_v$ so that $m_p = (x_1 - \lambda_1, \ldots, x_r - \lambda_r)$; clearly the image is maximal, and the map is $1:1$. We can then take the inverse map, which corresponds topologically to the immersion $k^r \to {k_v}^r$ and is clearly an homeomorphism onto its image. □

This shows that the properties of X reflect those of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$, a principle we'll use in several ways when proving Siegel's Theorem. Also observe that if k is not algebraically closed, the projection is $1:1$ only restricted to the rational points of X. (Example: the completion of $\mathbb{Q}$ with respect to the usual absolute value $v(q) = |q|$ is $\mathbb{R}$.)

Definition 2.2.4. An algebraic variety X over $k = \overline{k}$ equipped with the v-adic topology is *bounded* if it has a finite cover of open sets U_i, each contained in an affine subvariety and such that $U_i \cap X_0$ is bounded in the local induced metric. If k is not algebraically closed, we say X is bounded if $X \times_{\mathrm{spec}(k)} \mathrm{spec}(\overline{k})$ is.

Remark 2.2.12. *if an open cover U_i is made of bounded open subsets of an affine covering V_i, and T_j is another affine covering, The sets $U_i \cap T_j$ are bounded open sets of T_j.*

Our criterion for compactness is now clear:

Proposition 2.2.13. *Let X be an algebraic variety of positive dimension over k. the set $X(k)$ is compact with respect to the v-adic topology if k is complete, locally compact and X is bounded. If $k = \overline{k}$ the converse is also true.*

Proof. ($\Rightarrow$): let U_i be a finite open covering of $X(k)$ as in Definition (2.2.4). $\overline{U_i}$ is compact for all i, so $X(k)$ is covered by a finite number of compact sets, which implies $X(k)$ is compact.
($\Leftarrow$): if $X(k)$ is compact, let Ω be the set of open sets of $X(k)$ which are contained in an affine subvariety and bounded. As every $x \in X(k)$ has a neighbourhood in Ω, there is a finite subcovering of Ω, which implies $X(k)$ is bounded. Moreover, every U in Ω has compact closure, which means k is complete and locally compact. □

Projective varieties are naturally compact:

Proposition 2.2.14. *For all projective varieties over a complete, locally compact field k, $X(k)$ is compact.*

Proof. As all projective varieties are (topologically) closed subsets of ${\mathbb{P}_k}^n$ for some n, and the v-adic topology strictly contains the Zariski topology, it suffices to show that ${\mathbb{P}_k}^n$ is bounded when $k = \overline{k}$. Let us consider the sets $U_i = \{(x_0 : \ldots : x_n) | v(x_i) > v(x_j) \forall j \neq i\}$. U_i is contained in the affine chart $({\mathbb{P}_k}^n)_{(x_i)}$, where it corresponds to the unit cube, and is thus bounded. U_i is clearly open and $\bigcup_{i=0}^{n} U_i = {\mathbb{P}_k}^n$, which concludes the proof. □

The last preparation we need for the proof of Siegel's Theorem is about the points at infinity of an affine curve:

Proposition 2.2.15. *Let X be an affine curve over an algebraically closed field k, and let Σ_∞ be the closed subscheme of its points at infinity. Let $\tilde{X}$ be the projective completion of X. Then all points at infinity of $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$ are closed and extend to closed points of Σ_∞, and the map is $(1:1)$.*

Proof. As X is irreducible, Σ_∞ has dimention 0 as a closed subscheme and is then composed by a finite number of closed points. Now, $\Sigma_\infty \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$ is a closed subscheme of $\tilde{X} \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$ and $X \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v) \cup \Sigma_\infty \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v) = \tilde{X} \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$. Then $\Sigma_\infty \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$ must be the subscheme of the points at infinity of $\tilde{X} \times_{\mathrm{spec}(k)} \mathrm{spec}(k_v)$. Then its image by the projection π_1 is exactly Σ_∞, and, as it is contained in $\tilde{X}(k)$, we've already shown the projection is $(1:1)$ when restricted. □

This last proposition shows that completing our base field, in the case of dimension 1, "does not add any point at infinity", as geometric intuition suggest.

2.3 Proof of Siegel's Theorem

We have now developed all the instruments needed for a proof. Let's begin by citing the two main results we'll use in the proof:

Theorem 2.3.1 (Riemann-Roch)**.** *Let X be a curve of genus g over a field k, and let D be a divisor on X. We have:*

$$\dim_k H^0(X, \mathcal{O}_X(D)) = \dim_k H^0(X, \Omega_X \otimes \mathcal{O}_X(-D)) + \deg(D) + 1 - g.$$

Theorem 2.3.2 (Schimdt's Subspace Theorem)**.** *Let S be a proper, finite set of absolute values over k, and, for $v \in S$, $i \in 1, \ldots, n$, let $L_{i,v}$ be linear independent forms in n variables, with coefficents in $\overline{\boldsymbol{Q}}$. Let $\epsilon > 0$. The solutions $x \in {K_S}^n$ to the inequality:*

$$\prod_i \prod_v |L_{i,v}(x)|_v \leq H(x)^{-\epsilon}$$

all lie in a finite union of proper subspaces of k^n.

Proof. See [9] □

Actually, this is a generalization of the original *Schimdt's Subspace Theorem* by H. P. Schlickewei.
Now, let X be an affine curve over k, $\tilde{X}$ its projective completion, and $\Sigma_\infty = \{Q_1, \ldots, Q_r\}$ the set of its points at infinity, with $\sum_i [k(Q_i) : k] \geq 3$. Recall that we have shown (Remark 2.1.10) we only need to prove Siegel's theorem in this particular case. Our objective will be proving any Quasi-S integral subset of X is finite.

1. First, a few topological considerations.

   By Proposition (2.1.6), we may base change X to a field containing $k(Q_i)$ for all i, such that $[k(Q_i) : k] = 1$ and the numer of points at infinity r is greater or equal than 3.
   Now, suppose $\{p_j\}_{j \in \mathbb{N}}$ is an infinite sequence of Quasi-S integral points. As the p_j are rational points of $\tilde{X}$, for all $v \in S$ we have an infinite sequence of k_v rational points of $\tilde{X}_v$ (Proposition 2.2.11); as k_v is locally compact (this is true for any number field) and $\tilde{X}_v$ is projective, by (2.2.13) and (2.2.14) there is a converging subsequence q_j. As S is finite, we may suppose $q_j \to P_v \in \tilde{X}_v$ for all v.
   Observe there is at least an absolute value $v \in S$ such that $P_v \in$

$\{Q_1, \ldots, Q_r\}$, as any set of S-integral points of k^n bounded for all $v \in S$ is finite (it has bounded denominator, so we can multiply all elements by an algebraic integer to obtain a bounded subset of $\mathcal{O}_k$).

2. Now we'll use *Riemann-Roch* to construct a set of meromorphic functions on $\tilde{X}$ behaving in a controlled way at infinity.

   Let D_∞ be the divisor $\sum_{i=1}^r Q_i$, and $V_N = H^0(X, \mathcal{O}(ND_\infty)$. As $\deg(ND_\infty) = Nr$, by the *Riemann-Roch Theorem* $\dim(V_N) \geq Nr + 1 - g$ and we can choose $\overline{N}$ such that $d \doteq \dim(V_{\overline{N}}) \geq 2\overline{N} - 2$.
   Let now $\phi_1, \ldots, \phi_d$ be a base for $V_{\overline{N}}$. As $\mathrm{ord}(\phi_i) \geq 0$ for all $p \in X$, $\phi_1, \ldots, \phi_d \in \mathcal{O}_X(X)$ (Proposition 1.1.5), and we can choose them such that $\phi_i(q_j) \in K_S$ for all i and j. Let S' be the set of values in S such that $P_v \in \{Q_1, \ldots, Q_r\}$, $S'' = S \setminus S'$. For all $v \in S''$ the values $|\phi_i(q_j)|_v$ are uniformly bounded: this is because $f(p) = {\pi_v}^\sharp(f)(\pi^{-1}(p))$ for all rational points p of X and all $f \in \mathcal{O}_X(X)$, and ${\pi_v}^\sharp(f)$ is continuous for the $\tilde{v}$-adic topology of X_v, wich means $f(q_j) \to {\pi_v}^\sharp(f)(P_v)$ in the $\tilde{v}$-adic topology, which is the same as the v-adic topology when restricted to k.

   For $v \in S'$ let us consider $V_{l,v,\overline{N}}$ to be the subspace of V defined by $V_{v,l,\overline{N}} = \{f \in V_{\overline{N}} \mid \mathrm{ord}_{P_v}(f) \geq -\overline{N} + l - 1\}$. We have $V_{v,1,\overline{N}} = V_{\overline{N}}$, and $V_{v,l+1,\overline{N}} \subseteq V_{v,l,\overline{N}}$. We want to show that:

$$\dim(V_{v,l,\overline{N}}) - \dim V_{v,l+1,\overline{N}} \leq 1$$

   As $V_{v,l,\overline{N}} = H^0(X, \mathcal{O}_X(\overline{N}D_\infty - lp))$, by the *Riemann-Roch Theorem* we may write:

$$\dim_k H^0(X, \mathcal{O}_X(\overline{N}D_\infty - lp)) = \dim_k H^0(X, \Omega_X \otimes \mathcal{O}_X(-\overline{N}D_\infty + lp)) + \deg(\overline{N}D_\infty - lp) + 1 - g$$

   Let's compare this formula and the formula for $l + 1$:
   $\deg(\overline{N}D_\infty - lp - p) = \deg(\overline{N}D_\infty - lp) - 1$, and the dimension of $H^0(X, \Omega_X \otimes \mathcal{O}_X(-\overline{N}D_\infty + lp + p))$ is greater or equal then the dimension of $H^0(X, \Omega_X \otimes \mathcal{O}_X(-\overline{N}D_\infty + lp))$. This proves our statement.
   It is now possible for $v \in S'$ and $l \in \{1, \ldots, d\}$ to choose $\psi_{l,v}$ in $V_{v,l,\overline{N}}$ such that for all $v \in S'$ the functions $\psi_{1,v}, \ldots, \psi_{d,v}$ are linearly independent; for $v \in S''$ we define $\psi_{v,l} = \phi_l$.

3. We now turn our meromorphic functions to linear forms on k^n to apply the *Subspace Theorem.*

The values $\psi_i(p)$ are k-linear on $\phi_1(p), \ldots, \phi_d(p)$, so we can see them as linear forms in d variables: if $\psi_i = \lambda_1\phi_1 + \ldots + \lambda_d\phi_d$ the corresponding linear form will send $a_1e_1 + \ldots + a_de_d$ to $\lambda_1a_1 + \ldots + \lambda_de_d$. We're intrested in understanding their behavoir at the points at infinity.
For v in S', let t_v be a local parameter at P_v. Locally, if q is a rational point of X, we have $\mathrm{d}_v(q, P_v) \asymp t_v(q)$, and $\psi_{v,l} = {t_v}^{l-d-1}g_{v,l}$, with $g_{v,l}$ invertible in X_{P_v}, so that when evaluating at rational points near P_v, $g_{v,l} \asymp 1$. This shows $\psi_{v,l}(q) \asymp \mathrm{d}_v(q, P_v)^{l-d-1}$. Also, as the ϕ_i are uniformly bounded on $\{q_j\}_{j\in\mathbb{N}}$, $\psi_{v,l} \ll 1$ for all v in S''. The same argument shows that $|\phi_i(q)|_v \ll \mathrm{d}_v(q, P_v)^{-\overline{N}}$.
We have all the ingredients to conclude: let x_j be the vector of S-integers $(\phi_1(q_j), \ldots, \phi_d(q_j))$; the height $\mathrm{H}(x_j)$ is then asymptotically bounded by $\prod_{v\in S'} \mathrm{d}_v(q, P_v)^{-\overline{N}}$, as for all v outside of S $|x_j|_v \leq 1$, and for all v in S'' $|x_j|_v$ is bounded. Let us consider the product

$$\prod_{v\in S}\prod_{l=0,\ldots,d}|\psi_{v,l}(q_j)|_v$$

As $\sum_{l=1,\ldots,d} l - \overline{N} - 1 = \frac{d}{2}(d - 2\overline{N} - 1)$ by adding all the exponents we have:

$$\prod_{v\in S}\prod_{l=0,\ldots,d}|\psi_{v,l}(q_j)|_v \asymp \prod_{v\in S'}\mathrm{d}_v(q, P_v)^{\frac{d}{2}(d-2\overline{N}-1)}$$

Which yelds the (asymptotic) inequality:

$$\prod_{v\in S}\prod_{l=0,\ldots,d}|\psi_{v,l}(q_j)|_v \ll \mathrm{H}(x)^{-\frac{d(d-2\overline{N}-1)}{2\overline{N}}}$$

Now, recall we chose $d \geq 2\overline{N} + 2 \geq 2$; if we could turn the last asymptotic inequality to a pointwise inequality, we could apply the *Subspace Theorem* with $\epsilon = \frac{d}{2\overline{N}}$. To do so it is sufficient that $\mathrm{H}(q_j) \to \infty$, so that we can get the inequality for j large enough. As $d \geq 2$ and the ϕ_i are independent the points $x_j = (\phi_1(q_j), \ldots, \phi_d(q_j))$ are not all proportional, and by dividing by $\phi_1(q_j)$, which we may suppose is nonzero, we have $\mathrm{H}(x) = \mathrm{H}(\frac{1}{\phi_1(q_j)}x)$; as for all v $\sup_i |\frac{x_j(i)}{\phi_1(q_j)}|_v \geq 1$, if $\mathrm{H}(x_j)$ was bounded the norm of x_j would be bounded for all v and the x_j would be contained in a finite subset of k^d.
We can now apply the subspace theorem and conclude the points x_j are all contained in a finite union of proper subspaces of k^d: then all the x_j satisfy one of a finite number of linear equations; if they were infinite, an equation $a_1\phi_1(p) + \ldots + a_d\phi_d(p) = 0$ would hold for an infinite susbset of X, meaning $a_1\phi_1 + \ldots + a_d\phi_d = 0$. As the ϕ_i are independent, there must be only a finite number of x_j and thus the set q_j is finite.

Chapter 3

Hilbert's Irreducibility Theorem

3.1 Hilbert's Irreducibility Theorem

The second classical result we're going to prove is *Hilbert's Irreducibility Theorem*, still following a proof by Professor Umberto Zannier (from [10]). While *Siegel's Theorem* needed a little preparation just to be stated, we can state the irreducibility theorem right away:

Theorem 3.1.1 (Hilbert's Irreducibility Theorem)**.** *Let k be a finite extension of $\mathbb{Q}$, $F_1, \dots, F_r$ irreducible polynomials in $k[x_1, \dots, x_n, T_1, \dots, T_s]$, and $g \in k[T_1, \dots, T_s]$.*
There are infinite $(t_1, \dots, t_s) \in k^s$ such that $F_i(x_1, \dots, x_n, t_1, \dots, t_s)$ is irreducible in $k[x_1, \dots, x_n]$ for $i = 1, \dots, r$ and $g(t_1, \dots, t_s) \neq 0$.

So, the *Hilbert Irreducibility Theorem*, which we'll refer as *HIT* from now on, states that given a finite set of irreducible equations over k, there are always infinite possible specializations outside a given hypersurface that preserve irreducibility. While this is apparently a purely arithmetic matter, it's heavily connected to algebaric geometry, both in its applications and its possible proofs. We'll show here a proof based mostly on *Siegel's Theorem* and some basic algebraic geometry. First, let us see how we can gradually modify the statement to better fit the instruments we've developed in the previous chapter:

Proposition 3.1.2. *We can reduce to proving the case $s = 1, n = 1$.*

Proof. Clearly we can reduce to the case $s = 1$ by induction. Let's see how we can reduce to $n = 1$ too, restricting ourselves to the case $r = 1$ for simplicity:
the *Kronecker substitution* $\mathrm{S_d}$ is the morphism $k[x_1, \dots, x_n, T] \to k[y, T]$

defined by $x_i \to y^{d^i}, T \to T$. By the uniqueness of the d-adic expansion, S_d is a bijection beetween the sets of polynomials in $k[x_1, \ldots, x_n, T]$ with degree $\leq d$ in $x_1, \ldots, x_n$ and the set of polynomials in $k[y, T]$ with degree $\leq d^{n+1} - 1$ in y.
Now, let $F \in k[x_1, \ldots, x_n, T]$ be irreducible, $d \geq \deg(F)$, $\mathrm{S_d}(F) = \phi$. We factorize $\phi = \prod_{i=1,\ldots,l} \phi_i$, with ϕ_i irreducible in $k[y, T]$. Suppose we are able to choose $t \in k$ such that $\phi_i(y, t)$ is irreducible for all i. If $F_t = F(x_1, \ldots, x_n, t)$ is reducible, say $F_t = P_t Q_t$, then P_t (resp. Q_t) equals a partial product of the $\phi_i(t, y)$, and $\phi = \mathrm{S_d}(F) = P_T Q_T$. We may then choose $A, B \in k[x_1, \ldots, x_n, T]$ with degree $\leq d$ in all variables such that $\mathrm{S_d}(A) = P_T, \mathrm{S_d}(B) = Q_T$.
If the product AB had degree $\leq d$ in all variables, we would have $F = AB$. As F is irreducible, there must be a monomial of AB whose degree is $> d$ in a variable x_j. The coefficient of this monomial belongs to $k[T]$. Suppose we may choose t with the additional property that t is not a zero of any of those (finite) coefficients, for all possible choices of partial products of $\prod_{i=1,\ldots,l} \phi_i$. Then $\mathrm{S_d}(P_t) = \mathrm{S_d}(A_t), \mathrm{S_d}(Q_t) = \mathrm{S_d}(B_t)$, so $\mathrm{S_d}(F_t) = \mathrm{S_d}(A_t B_t)$ which is impossible as $A_t B_t$ is still of degree $> d$ in a variable. Then, for all t having both these properties, F_t is irreducible. The *HIT* (with $n = 1, s = 1, r = 1$) implies we can choose infinite such t outside the set of zeros of any given $g \in k[T]$.

□

We are now ready to link the *HIT* directly with the theory of diophantine equations:

Proposition 3.1.3. *Suppose k is a field such that for all finite sets $\{g_i\}_{i=1,\ldots,r}$ of irreducible polynomials in $k[y, T]$ there are infinite $t \in k$ such that $g_i(y, t)$ has no zeros in k for all i, then the* HIT *holds for k. We call such fields* Hilbertian.

Proof. Let F be an irreducible polynomial in $k[y, T]$. Let Ω be a decomposition field for $F = 0$ over $k(T)$, such that $F = c(T)(y - \alpha_1) \ldots (y - \alpha_r)$ with $\alpha_i \in \Omega$; as the α_i are integral over $k\left[T, c(T)^{-1}\right]$ we may extend the morphism $T \to t \in k$ for all t outside of a finite set S. We have:

$$f \doteq F(y, t) = c(t) \prod_{i=1,\ldots,r} (y - \alpha_i(t))$$

if f is reducible, a proper subset of the product on the right has coefficients in k. Let $J = \{1, \ldots, d\}$ be this subset, and let us consider $\prod_{i \in J} (y - \alpha_i)$. As F is irreducible, this product must have at least a coefficient not in $k[T]$; we name it ω_j. Let $g_j \in k(T)[y]$ be its minimal polynomial over $k(T)$. Obviosly g_j is irreducible and of degree > 1. On the other hand, g_j has the zero $\omega_j(t) \in k$. Multiplying g_j by its denominator, we have an irreducible polynomial $G_j \in k[y, T]$ of degree > 1 such that $G_j[y, t]$ has a zero in k.

Then if we can choose $t \in k$ such that for all possible choices of subproducts and coefficients $G_j(t, y)$ has no zeros in k, f must be irreducible. □

Now, suppose we have a polynomial $G(y, T) \in k[y, T]$, and let $t \in k$. A zero of $G(y, t)$ corresponds to a rational point (y_t, t) of the closed subvariety $X \doteq V(G) \subset \mathbb{A}^2{}_k$; if we consider the morphism $f_T : X \to \mathbb{A}^1{}_k$ induced by T, we have $t \in f_T(X(k))$. Then, given a finite set of irreducible polynomials $G_i \in k[y, T]$ of degree > 2 the last proposition can be restated as:

$$\mathbb{A}^1{}_k(k) \setminus \cup_i f_T(X_i(k)) \text{ is infinite.}$$

The maps $f_T : X_i \to \mathbb{A}^1{}_k$ are all of degree equal to or greater than two, as $k[y, T]/(G_i)$ has rank ≥ 2 as a $k[T]$ module. Recall now that any finite set of k-rational points is a closed subvariety of $\mathbb{A}^1{}_k$. This suggests our next generalization:

Definition 3.1.1. Let X be an algebraic variety over k. A subset of $V(k)$ is *thin* if it is covered by a finite union of:

- $V(k)$, where V is a proper closed subvariety of X.
- $f(Y(k))$, where f is a finite morphism of algebraic varieties of degree greater or equal than two.

Remark 3.1.4. *With our new terminology, if $\mathbb{A}^1{}_k(k)$ or equivalently $\mathbb{P}^1{}_k(k)$ is not thin, k is Hilbertian.*

Proposition 3.1.5. *If there is any variety X such that $X(k)$ is not thin, $\mathbb{P}^1{}_k$ is not thin and k is Hilbertian.*

Proof. It suffices to show that if $\mathbb{P}^1{}_k$ is thin, $X(k)$ is thin for any algebraic variety over k. Let $\mathcal{C}_1, \ldots, \mathcal{C}_r$ be algebraic varieties of dimension 1 over k with projections $\rho_1, \ldots, \rho_r$ as in Definition (3.1.1), $\{P_1, \ldots, P_s\}$ the (finite) complementary of $\mathbb{P}^1{}_k \setminus \cup_{i=1,\ldots,r} \rho_i(\mathcal{C}_i(k))$. If X is another algebraic variety over k, after chosing any morphism $f : X \to \mathbb{P}^1{}_k$ (these correspond $1:1$ to mermorphic functions over X, and there is always one due to the *Riemann-Roch* theorem), we consider the fibered products $\tilde{\mathcal{C}}_i \doteq X \times_{\mathbb{P}^1{}_k} \mathcal{C}_i$. The first projection $\pi_1 : \tilde{\mathcal{C}}_i \to X$ is a finite morphism of degree $\geq \deg(\pi_i)$.
Now, let P be a rational point of X. $f(P)$ is rational. If $f(P) \in \rho_i(\mathcal{C}_i(k))$, the two inclusions $P \cong \text{spec}(k) \to X, P \to \mathcal{C}_i$ give rise to a commutative diagram, and by the universal property of fibered products there is an inclusion $R \cong \text{spec}(k) \to \tilde{\mathcal{C}}_i$ such that $\pi_1(R) \doteq \tilde{\rho}_i(R) = P$. Then we have $\cup_{i=1,\ldots,r} \tilde{\rho}_i(\tilde{\mathcal{C}}_i(k)) \supseteq X(k) \setminus f^{-1}(\{P_1, \ldots, P_s\})(k)$. As $f^{-1}(\{P_1, \ldots, P_s\})(k)$ is a proper closed subvariety of X, $X(k)$ is thin.

□

We can now move on to proving the *HIT*. We'll show that no finite number of curves over a number field k can cover ${\mathbb{P}^1}_k(k)$; it will suffice to show the complementary of their images contains infinite *integral* points, by means of *Siegel's Theorem*, and of course, the omnipresent *Riemann-Roch Theorem*.

Proposition 3.1.6. *Let $\mathcal{C}_i i = 1, \dots, r$ be curves over a number field k, $\rho_i : \mathcal{C}_i \to {\mathbb{P}^1}_k i = 1, \dots, r$ finite morphisms of degree greater than one. There are infinitely many* integral *points of ${\mathbb{A}^1}_k$ outside the union of the images of $\mathcal{C}_1(k), \dots, \mathcal{C}_r(k)$.*

We'll first prove a few lemmas:

Lemma 3.1.7. *we may suppose the $\mathcal{C}_i$ are projective and normal.*

Proof. Let X_i be an affine open subscheme of $\mathcal{C}_i$; then $\mathcal{C}_i$ is birational to its projective closure $\tilde{X_i}$; we may always extend a morphism of affine varieties to their projective completions, so we have a morphism $\tilde{X_i} \to {\mathbb{P}^1}_k$. We may further compose with the normalization morphism ${\tilde{X_i}}^\nu \to \tilde{X_i}$. The new map $\tilde{\rho_i}$ is clearly of the same degree as ρ_i. As the rational points of X_i are the same as those of $\tilde{X_i}$, and the inverse image of a rational point of $\tilde{X_i}$ is a rational point of ${\tilde{X_i}}^\nu$, clearly $\mathcal{C}_i$ and ${\tilde{X_i}}^\nu$ are the same with respect to Proposition (3.1.6). □

Lemma 3.1.8. *We may suppose the $\mathcal{C}_i$ are of genus 0 and the inverse image of ∞ has degree at most two.*

Proof. Let $U_0 \cong {\mathbb{A}^1}_k$ be the affine open subscheme ${\mathbb{P}^1}_k \setminus \infty$. We have a morphism of affine varieties (recall that for a finite morphism the inverse image of an affine subscheme is affine) $\mathcal{C}_i \setminus \rho^{-1}(\infty) \to U_0$; we're interested in studying the rational points of $V_i \doteq \mathcal{C}_i \setminus \rho^{-1}(\infty)$ whose image is an integral point of U_0. By Proposition (2.1.2), those points are Quasi-integral points of V_i (i.e. Quasi-S integral points with $S = M_\infty$). We may then restrict to the curves such that V_i has infinite Quasi-integral points. The *Siegel's Theorem* then implies $g(\mathcal{C}_i) = 0$ and $\deg(\rho^{-1}(\infty)) \leq 2$. □

Lemma 3.1.9. *We may suppose the $\mathcal{C}_i$ are isomorphic to ${\mathbb{P}^1}_k$.*

Proof. As an application of the *Riemann-Roch Theorem*, we'll show that any projective curve $\mathcal{C}$ of genus zero over k having at least a rational point is isomorphic to ${\mathbb{P}^1}_k$. Let P be a rational point of $\mathcal{C}$: as a divisor, P has degree 1. By *Riemann-Roch*, $\dim_k(\mathrm{H}^0(\mathcal{C}, \mathcal{O}(P)) = 1 + \deg(P) + \dim_k(\mathrm{H}^0(\mathcal{C}, \Omega_\mathcal{C} \otimes \mathcal{O}(-P))$; as $\Omega_\mathcal{C} \otimes_k \mathcal{O}(-P)$ has degree -3, $\dim_k(\mathrm{H}^0(\mathcal{C}, \Omega_\mathcal{C} \otimes \mathcal{O}(-P)) = 0$ and $\dim_k(\mathrm{H}^0(\mathcal{C}, \mathcal{O}(P)) = 2$.
An invertible sheaf with two global sections s_0, s_1 gives rise to a morphism $T : \mathcal{C} \to {\mathbb{P}^1}_k$ if the two sections are never both zero at a point $Q \in \mathcal{C}$. Suppose this happens: then we would have $\mathrm{H}^0(\mathcal{C}, \mathcal{O}(P)) = \mathrm{H}^0(\mathcal{C}, \mathcal{O}(P - Q))$, as they

are both generated by $\{s_0, s_1\}$. Let Q be such a point. If $k(Q)/k > 1$ then $\deg(P-Q) < 0$ and $\dim_k(\mathrm{H}^0(\mathcal{C}, \mathcal{O}(P-Q)) = 0$, while if Q is a rational point, $\Omega_{\mathcal{C}} \otimes_k \mathcal{O}(-P+Q)$ has degree -2 and we may argue as before to conclude $\dim_k(\mathrm{H}^0(\mathcal{C}, \mathcal{O}(P-Q))) = 1$. So, we have a morphism $T : \mathcal{C} \to {\mathbb{P}^1}_k$. As T sends $\mathcal{O}_{{\mathbb{P}^1}_k}(1)$ to $\mathcal{O}(P)$, by the formula $\deg(T^*(L)) = \deg(T)\deg(L)$ the degree of T is 1, which implies T is an isomorphism by Proposition (1.6.11). □

This lemma has the added value of giving us a clearer view of the strenght of *Siegel's Theorem*:

Remark 3.1.10. *Let X be an affine curve of genus zero over k. If X has a single point at infinity, X has an infinite Quasi-integral set. If X has two points at infinity, there is an extension k'/k of degree at most 4 such that $X \times_{\mathrm{spec}\, k} \mathrm{spec}(k')$ has an infinite Quasi-integral set.*

Proof. Let $\tilde{X}$ be the projective completion of X. Now, if X has a single point at infinity, this is a rational point and X is isomorphic to ${\mathbb{P}^1}_k \setminus \infty = {\mathbb{A}^1}_k$, and thus has an infinite set of Quasi-integral points. If X has two (geometrical) points p_1, p_2 at infinity, there are two cases.

- If p_1, p_2 are rational, $\tilde{X}$ is isomorphic to ${\mathbb{P}^1}_k$ over k, and by a projective change of coordinates we may suppose $p_1 = 0, p_2 = \infty$. Then $X = \mathrm{spec}(k\left[x, x^{-1}\right])$, and we just need to base change to a field k' such that ${\mathcal{O}_{k'}}^*$ is infinite, so that the points (α, α^{-1}) will form an infinite integral set. To do so, we just need to add $\sqrt{2}$ to our field, so that $(\sqrt{2}-1)^n$ will belong to ${\mathcal{O}_{k'}}^*$ for all n.
- If p_1, p_2 are the inverse images of a single point p of degree 2, then we just need to base change to $k(p)(\sqrt{2})$ and apply the same reasoning as before.

□

Now that we have greatly reduced the possible cases, we may proceed to the final part of the proof, after citing one last result:

Definition 3.1.2. Let k be a number field. The *norm* $\|\alpha\|$ of $\alpha \in k$ is the maximum of its archimedean absolute values. We'll call $B_k(m)$ the set $\{\alpha \in \mathcal{O}_k \mid \quad \|\alpha\| \leq m\}$.

Theorem 3.1.11. *The set $B_k(m)$ is finite and its rate of growth is asymptotic to $m^{[k:\mathbb{Q}]}$.*

Proof. See [2]. □

Proof of Proposition (3.1.6). We have reduced to two cases:

1. $\mathcal{C} = \mathbb{P}^1{}_k, \deg(\rho^{-1}(\infty)) = 1$

   Then $\rho^{-1}(\infty)$ as a divisor is effective and has degree one, so it is a single k-rational point. We have then an affine morphism $\mathbb{A}^1{}_k \to \mathbb{A}^1{}_k$ of degree ≥ 2. By Proposition (2.1.2) the set of points which are rational and have integral image is a Quasi-integral set of $\mathbb{A}^1{}_k$, so we may suppose they are integral by multiplying by a nonzero constant, which does not change the degree of our map. Now, a map $\mathbb{A}^1{}_k \to \mathbb{A}^1{}_k$ of degree $d \geq 2$ is induced by a polinomyal f of degree d, and clearly $\|f(P)\| \asymp \|P\|^d$, so that the number of integral points such that $\|f(P)\| \leq M$ in $f(\mathbb{A}^1{}_k(k))$ is asymptotically bounded by $\mathrm{B}_k(M)^{\frac{1}{d}}$.

2. $\mathcal{C} = \mathbb{P}^1{}_k, \deg(\rho^{-1}(\infty)) = 2$

   By base changing to an extension k' of k of degree at most two, we may suppose $\rho^{-1}(\infty) = \{P, Q\}$, with $\{P, Q\} \subseteq \mathbb{P}^1{}_{k'}(k')$. Clearly the fact that $\mathbb{P}^1{}_{k'}(k') \setminus \mathcal{C} \times_{\mathrm{spec}(k)} \mathrm{spec}(k')$ is infinite does not imply the same for k, but we'll find an asymptotic inequality strong enough to prove our claim.
   By applying a projective transformation we may suppose $P = 0, Q = \infty$, so that we have a morphism $\mathbb{A}^1{}_{k'} \setminus 0 \to \mathbb{A}^1{}_{k'}$, and again we may suppose the rational inverse images of integral points are integral. A morphism $\mathbb{A}^1{}_{k'} \setminus 0 \to \mathbb{A}^1{}_{k'}$ is induced by a rational function $f \in k\left[x, x^{-1}\right]$, which we may always write as $f_1(x) + f_2(x^{-1})$, with $\max(\deg(f_1), \deg(f_2)) \geq 2$.
   Now, we may explicitly note that if P is an integral point of $\mathbb{A}^1{}_{k'} \setminus 0$, $P = (t, \frac{1}{t})$, and both t and $\frac{1}{t}$ are integral, so that t is a unit of the integral closure of $\mathbb{Z}$ in k'. As the group $\mathcal{O}^*_{k'}$ is finitely generated for all number fields, there is $c \in \mathbb{N}$ such that the number of integral points of $\mathbb{A}^1{}_{k'} \setminus 0$ whose norm is $\leq M$ is asymptotically bounded by $\log(M)^c$, and again the number of integral points in the image of $\mathbb{A}^1{}_{k'} \setminus 0 \to \mathbb{A}^1{}_{k'}$ is asymptotically bounded by $\log(\mathrm{B}_{k'}(M))^d$. As the integral points $\leq M$ of k' are asymptotically bounded by the square of those of k, this inequality implies our claim for k too.

□

It's intresting to notice that our proof also implies that the subset of integrals of k for which the *HIT* "fails" is quite a small one:

Remark 3.1.12. *Let $f_1, \ldots, f_r \in k\left[x_1, \ldots, x_r, y\right]$ be irreducible. The subset $D(f)$ of $\mathcal{O}_k$ defined by $\{\alpha \in \mathcal{O}_k \mid \exists 1 \leq i \leq r, f_i(x_1, \ldots, x_r, \alpha)$is reducible$\}$ is cointained in a thin subset of $\mathbb{A}^1_k$ and there is $C(f) \in \mathbb{N}$ such that* $\mathrm{card}(D \cap B_k(n)) \leq C(f) B_k(n)^{\frac{1}{2}}$.

Proof. We have seen in the proof of Proposition (3.1.3) that the set $D(f)$ is contained in a thin subset of $\mathbb{A}^1_k$, and the estimate of its cardinality is given in the last part of the *HIT*'s proof. □

While the growth of "bad" integers for f is bounded by the square root of $C(f)B(n)_k$, we cannot hope to get a uniform bound for $C(f)$, as the next propositions shows:

Proposition 3.1.13. *The constant $C(f)$ may assume arbitrarily large values.*

Proof. First we'll show a simple example for $k = \mathbb{Q}$.
Let $\{P_i\}_{i\in N}$ be the set of postive prime numbers, let $\mathrm{j} : \{1, \dots, 2^n\} \to \{-1, 1\}^n$ a bijection and let $f_n(x, T) \in \mathbb{Z}[x, T]$ be defined by the product:

$$f(x, T) = \prod_{i=1,\dots,2^n}(x - (\mathrm{j}_i(1)\sqrt{P_1 T} + \dots + \mathrm{j}_i(n)\sqrt{TP_n}))$$

f has coefficients in $\mathbb{Z}$ as the product is clearly in $\mathbb{Z}(\sqrt{P_1}, \dots, \sqrt{P_n})\left[x, \sqrt{T}\right]$, and is fixed by the Galois group of $\mathbb{Q}(T)(\sqrt{TP_1}, \dots, \sqrt{TP_n})/\mathbb{Q}(T)$.
f must also be irreducible over $\mathbb{Q}$ as none of the subproducts is defined over $\mathbb{Q}(T)$ (this is because the Galois group is transitive on the linear factors): if f would factorize over $\mathbb{Q}$, it would factorize over $\mathbb{Q}(T)$, which is not possible.
Now, let H be a proper subgroup of $\mathrm{Gal}(\mathbb{Q}(T)(\sqrt{TP_1}, \dots, \sqrt{TP_n})/\mathbb{Q}(T))$: if H wouldn't fix any partial product of f, H would be transitive on the linear factors of f, which in this case, as our extension is generated by any root of f, would imply that $H = \mathrm{Gal}(\mathbb{Q}(T)(\sqrt{TP_1}, \dots, \sqrt{TP_n})/\mathbb{Q}(T))$.
Then there are two subproducts h, g fixed by H, which implies their coefficients belong to the subextension fixed by H. By the Galois correspondence, we can use this to obtain factorizations of f with coefficients in any given subfield $\mathbb{Q}(T)(\sqrt{TP_1}, \dots, \sqrt{TP_n}) \supset K \supset \mathbb{Q}(T)$. In particular, we consider the subfields $\mathbb{Q}(T)(\sqrt{TP_i})$; if $f = hg$, with h, g in $\mathbb{Q}(T)(\sqrt{TP_i})$ then this factorization would hold true whenever TP_i is a perfect square: this set grows as $\sqrt{n}{P_i}^{-1}$.
We may then conclude that $C(f) \geq \sum_{i=1,\dots,n} {P_i}^{-1}$. As the sum of the inverses of prime number diverges, we can conclude that for all M there is an irreducible polynomial $f \in \mathbb{Z}[x, T]$ such that $c(f) \geq M$.

□

Notice that for a generic number field K the usual estimate $\sum_{i=1,\dots n} {P_i}^{-1} \asymp \log(\log(n))$ is no longer sufficient to obtain arbitrary values of $C(f)$, as the subset of $\mathcal{O}_K$ such that $\sqrt{\alpha P_i} \in \mathcal{O}_K$ grows as $\frac{\sqrt{B_K(n)}}{{P_i}^{[K:\mathbb{Q}]}}$. Let us now see how we can slightly refine our example to be able to choose any number field K, and also get a better estimate:

Proposition 3.1.14. *Let $M(d)$ be the supremum of $C(f)$ restricted to irreducible polynomials of degree $\leq d$. Then $M(d) \geq [\log_2(d)]$.*

Proof. We're going to use the same construction as before, only this time we'll be using $\sqrt{P_i + T}$ rather than $\sqrt{TP_i}$. The difference is now we need to show the extensions $K(T)/K(T)(\sqrt{P_i + T})$ are all linearly disjoint, a

thing which was obvious in the previous proposition. To do this, we'll show $K(T)(\sqrt{P_1+T},\dots,\sqrt{P_{i+1}+T})/K(T)(\sqrt{P_1+T},\dots,\sqrt{P_i+T}) \doteq L_{i+1}/L_i$ is not trivial, and thus has degree 2.
We'll proceed by induction. The base step is clear: $K(T)/K(T)(\sqrt{P_1+T})$ has degree 2. Now, suppose $[L_i : K(T)] = 2^i$, and thus its Galois group is $(\mathbb{Z}/2\mathbb{Z})^i$; if $\sqrt{P_{i+1}+T}$ belongs to L, then it generates a subfield of degree two. Let's see what kind of elements of L generate a subfield of degree two. A generic element of L can always be written this way:

$$l = Q_1(T)^{-1} \sum_{A\in\mathcal{P}\{1,\dots,i\}} Q_A(\prod_{j\in A} \sqrt{P_j+T})$$

Where Q_1, Q_A are all in $K[T]$. For a subgroup of $\mathrm{Gal}(L_{i+1}/K(T))$ to fix it, it must fix $\pi_A \doteq \prod_{j\in A}\sqrt{P_j+T}$ for all A such that Q_A is not 0. Now, clearly π_A generates an extension of degree 2 of $K(T)$, and thus it is fixed by a subgroup H_A of index two in $\mathrm{Gal}(L_{i+1}/K(T))$. As these subgroups are all different, the only way k can be fixed by a subgroup of index two is if all Q_A are zero except for two: the one relative to the empty set and another one.
We have shown that if $\sqrt{P_{i+1}+T}$ belongs to L_{i+1}, it must belong to the subfield generated by π_A for some $A \in \mathcal{P}(\{1,\dots,i\})$. This would imply we can write $\sqrt{P_{i+1}+T} = Q_1(\prod_{j\in A}\sqrt{P_j+T}) + Q_2$, with Q_1, Q_2 in $\mathbb{Q}(T)$; this is not possible as their squares are different, as we can see multiplying by their denominator and using the fact that $K[T]$ is a unique factorization domain.
We may finally proceed as we did previously, with the only difference that this time the factors $\sqrt{P_i+T}$ take on integral values on a subset whose asymptotic growth is exactly $\sqrt{B_K(n)}$; as the degree of our polynomial is 2^n, given a degree d, consider the maximum m such that $2^m \leq d$; we have $[\log_2(d)] = m$. Then there is a polynomial $f_m \in \mathbb{Q}[x,T]$ of degree lower than d such that $C(f_m) \geq m$, which is exactly our claim.

□

3.2 Universal Hilbert sets

In the last section we've seen that the proof of the *Irreducibility Theorem* boils down to the case of two variables and integral points of $\mathbb{A}^1_k$. After noticing that, given a finite family of polynomials, the set D of "bad" integers is quite small it's only natural to step further and ask whether there are subsets of $\mathcal{O}_k$ which are "good" for all choices of polynomials, except possibly for a finite number of elements. In this section we'll see the answer is positive, we'll prove the existence of a "very large" such set, and we'll explicitly show a much smaller one.

Definition 3.2.1. An infinite subset H of $\mathcal{O}_k$ is a *Universal Hilbert set* (with respect to k) if given any irreducible polynomial $f \in k[x, y]$, there is a finite subset $K \subset H$ (depending on f) such that $f(x, \alpha_n)$ is irreducible for all $\alpha \in K^c$.

Recall now we just proved that, given a polynomial f, the set $D(f)$ grows at most as $\mathrm{O}(\sqrt{(}B_k(N)))$; given a numbering $\{f_i\}_{i\in\mathbb{N}}$ of the irreducible polynomials in $k[x, y]$, we may try to construct a universal set by showing the existence of a set D such that $D(f_i) \setminus D$ is finite for all f_i. If the complementary of D is infinite, it is a *Universal Hilbert set* by construction. This was done by Yuri Bilu (in [11]) and, separately, by Umberto Zannier and Pierre Dèbes (in [12]) in 1996. Here we'll follow Yuri Bilu's proof, which gives a somewhat stronger numerical estimate.

Theorem 3.2.1. *Given a number field k, There is a* Universal Hilbert set *of asymptotic density 1.*

Proof. As the elements of $k[x, y]$ are countable, we may choose a numbering $\{f_i\}_{i\in\mathbb{N}}$ of the set of all irreducible polynomials in $k[x, y]$.
Let $\psi : \mathbb{R}_+ \to \mathbb{R}_+$ be a continuous, increasing bijection. Let $N_\psi(f_i)$ be $\max(i, \psi^{-1}(C(f_1) + \ldots + C(f_i)))$, where $C(f_i)$ is the constant defined in Remark (3.1.12). Now let $\tilde{D}_\psi(f_i)$ be the set $\{\alpha \in D(f_i) \mid \|\alpha\| \geq N_\psi(f_i)\}$, and $\tilde{D}_\psi = \cup_{i\in\mathbb{N}}\tilde{D}_\psi(f_i)$. Now, set $H_\psi = \mathcal{O}_k \setminus \tilde{D}_\psi$. Clearly if H_ψ is infinite, it is a *Universal Hilbert set*. We'll proceed to show that. for all ψ such that $\psi \in \mathrm{o}(\sqrt{B_k})$, H_ψ has asymptotic density 1.
We observe at once that the sequence $N_\psi(f_i) \doteq N_{\psi,i}$ is increasing for all ψ, so given $M \geq N_{\psi,1}$ there is $r \in \mathbb{N}$ such that $N_{\psi,r} \leq M < N_{\psi,r+1}$. So:

$$B_k(M) \cap \tilde{D}_\psi = B_k(M) \cap (\cup_{1\leq i\leq r}\tilde{D}_\psi(f_i)) \subseteq B_k(M) \cap (\cup_{1\leq i\leq r}D(f_i)).$$

This implies:

$$\|B_k(M) \cap \tilde{D}_\psi\| \leq (C(f_1) + \ldots + C(f_r))\sqrt{B_k(M)}$$

By construction, we have $C(f_1) + \ldots + C(f_r) \leq \psi(M)$, so:

$$\|B_k(M) \cap \tilde{D}_\epsilon\| \leq \psi(M) B_k(M),$$

which in turn implies the asymptotic density of $\tilde{D}_\psi$ is zero for all ψ such that $\frac{\psi(n)}{B_k(n)} \to 0$, thus H_ψ has density 1. □

It's interesting to notice that by choosing ψ we may decrease the growth of ${H_\psi}^c$ as close as we want to $\sqrt{B_k(n)}$ (and this is the best we can hope, as we've seen the constants $C(f_i)$ are not bounded). The implicit cost of this process is that, given an irreducible polynomial f_i, the subset of H_ψ which is "bad" for f_i will grow proportionally to the growth of the inverse of ψ.

Now we'll briefly explore the limits of such a large *Hilbert Universal set*; namely, given any finite set, H must miss infinitely many of its translates.

Proposition 3.2.2. *Let H be a* Hilbert Universal set *with respect to k, and $A \subset \mathcal{O}_k$ a finite set. Then H can have nonempty intersection with only finitely many translates of A in the form $P(\alpha)+A$, with $P \in \mathcal{O}_k[x]$ of degree ≥ 2, $\alpha \in \mathcal{O}_k$.*

Proof. The proof is immediate: if H intersects $P(\alpha) + A$ for infinitely many α, there is $a \in A$ such that $a + P(\alpha) \in H$ for infinitely many α. For all such numbers the polynomial $P(x) - y - a$, which is irreducible, factorizes as $Q(x)(x - \alpha)$, thus H is not a *Hilbert Universal set.* □

Then, if we consider $A = B_k(n)$, we see any *Hilbert Universal set* must miss infinitely many arbitrarily large "segments" of integers (the word "segment" is motivated by the fact that if $k = \mathbb{Q}$, then $B_k(n) = \{-n, \ldots, n\}$).

While it was quite easy to prove there are very large *Hilbert Universal sets*, our proof is higly ineffective. As we'll see, showing that an actual sequence of numbers is Hilbert Universal can be very difficult, and to date there are no explicit *Hilbert Universal sets* of positive asymptotic density. Here we'll show a family of *Hilbert Universal sets* in the form of sequences with exponential growth, mostly following a sketched proof of U.Zannier and P.Dèbes from [12] relative to the case $h_n = 2^n(n^3 + 1)$. This case was already proven by M.Yasumoto using nonstandard arithmetics, while our proof will be totally based on classical diophantine arguments.

First, we state the two main theorems we'll use:

Theorem 3.2.3 (Generalized Roth's Theorem)**.** *Let k be a number field, S a finite set of normalised absolute values containing all the archimedean ones. For $v \in S$, let α_v be elements of $\overline{\mathbb{Q}} \cup \infty$, and let $\epsilon > 0$. Then there are at most finitely many numbers $\beta \in k$ such that:*

$$\prod_{v\in S} |\alpha_v - \beta|_v \leq \mathrm{H}(\beta)^{-2-\epsilon}$$

Where $|\infty - \beta|_v \doteq |\frac{1}{\beta}|_v$.

Proof. See [5]. □

The second theorem is actually a simplified version of a stronger result due to Le Veque:

Theorem 3.2.4 (Le Veque)**.** *Let k be a number field, S a finite set of absolute values containing all the archimedean ones. If $f \in k[x]$ has only simple zeros and $\deg(f) > 2$, the equation $f(x) = y^m$ has only a finite number of solutions in K_S for $m \geq 2$.*

Proof. See [13]. □

By *Siegel's Theorem* and Remark (3.1.10), this is tantamount to saying the normalization of the projective closure of $\mathrm{spec}(k[x,y]/\langle y^n - f(x)\rangle)$ always has genus ≥ 1 or at least three points at infinity when the conditions of the theorem are met.

We are now ready to begin the (quite long) proof:

Proposition 3.2.5. *Let k be a number field, P a prime element of $\mathcal{O}_k$ such that $\min_{v\in M_\infty}(|P|_v) > 1$, and $F \in \mathcal{O}_k[x]$ a polynomial with only simple zeros, of degree greater than two. Then $H = \{F(n)P^n\}_{n\in\mathbb{N}}$ is a* Universal Hilbert set*.*

Proof. It suffices to show that H has finite intersection with any thin subset of ${\mathbb{P}^1}_k$. So, let $f : {\mathbb{P}^1}_k \to {\mathbb{P}^1}_k$ be a morphism of degree two or more. As we recall from proving the *HIT*, there are two cases:

1. f has two poles.

   As we did before, by going to an extension $k' : k$ of degree at most two, we may suppose the poles are defined over k', and more precisely the poles are 0 and ∞. Recall that we may also modify f so that the inverse images of integral points are all units of $\mathcal{O}_k$, and $f = f_1(t) + f_2(\frac{1}{t})$. Then, let t_n be a sequence of units such that $f(t_n) \in H$; as $|F(n)P^n|_v \nearrow \infty$ for all archimedean absolute values, for all $v \in M_\infty$ the sequence $|t_n|_v$ cannot be bounded both from above and from below.
   Now, let $D = [k' : \mathbb{Q}]$ and let $M_\infty = \{v_1, \ldots, v_D\}$. We may choose a subsequence $\{q_{1,n}\}$ such that either $|q_{1,n}|_{v_1} \nearrow \infty$ or $|q_{1,n}|_{v_1} \searrow 0$, then do the same for $v_2, \ldots, v_D$ obtaining a sequence $\{q_{D,n}\}$ such that for all archimedeans values the sequence has either 0 or ∞ as a limit. We'll call this sequence $\{q_n\}$ for simplicity.

Let now ${M_\infty}^+$ be the set of archimedean absolute values such that $q_n \nearrow \infty$, ${M_\infty}^-$ the set of those such that $q_n \searrow 0$. By symmetry, suppose ${M_\infty}^+ \neq \emptyset$. By moving the constant term of f_2 to f_1, we have $f_2(\frac{1}{q_n}) = \frac{1}{q_n} g(\frac{1}{q_n})$; as the order of growth of $|f_1(q_n)|_v$ is a power of that of $|q_n|_v$, we have $|f_2(\frac{1}{q_n})|_v \leq C|P|^{-\epsilon n'}$ for all $v \in {M_\infty}^+$, where n' is such that $f_1(q_n) + f_2(\frac{1}{q_n}) = F(n')P^{n'}$.

After this preparation, we can consider the fraction $\frac{f_1(q_n)}{F(n')P^(n')}$; for all $v \in {M_\infty}^+$, we have $|1 - \frac{f_1(q_n)}{F(n')P^{n'}}|_v = |\frac{f_2(\frac{1}{q_n})}{F(n')P^{n'}}|_v \leq C|P|^{-\epsilon n'}|P|_v{}^{-n'}$.

For all $v \in {M_\infty}^-$, the value of $|f_1(q_n)|_v$ is bounded, so $|\frac{f_1(q_n)}{F(n')P^{n'}}|_v \leq C_v|P|_v{}^{n'}$.

With these premises, we want to apply the *Generalized Roth's Theorem* choosing $\beta_n = \frac{f_1(q_n)}{F(n')P^(n')}$, $\alpha_v = 1$ for all v in ${M_\infty}^+$, $\alpha_v = 0$ for all v in ${M_\infty}^-$, and finally $\alpha_v = \infty$ for all euclidean values extending $|\quad|_P$.

To estimate the value of $\mathrm{H}(\frac{f_1(q_n)}{F(n')P^{n'}})$, first we notice that for all archimedean values, $\frac{f_1(q_n)}{F(n')P^{n'}}$ has either 1 ir 0 as a limit, which implies the product $\prod_{v \in M_\infty} \max(1, |\frac{f_1(q_n)}{F(n')P^{n'}}|_v)$ is eventually bounded by any constant greater than one, say 2. Next we observe that all the contribution from euclidean values not extending $|\quad|_P$ comes from the factor $F(n')$ and is thus asymptotically bounded by $n'^{\deg(F)}$; name now M_P the set of absolute values extending $|\quad|_P$ (this set has at most two elements): we have shown that $\mathrm{H}(\frac{f_1(q_n)}{F(n')P^{n'}})$ is asymptotically bounded by:

$$n'^{\deg(F)} \prod_{v \in M_P} \max(1, |\tfrac{f_1(q_n)}{F(n')P^{n'}})|_v) = n'^{\deg(F)} \prod_{v \in M_P} |\tfrac{f_1(q_n)}{F(n')P^{n'}}|_v.$$

This is in turn bounded by:

$$n'^{\deg(F)} \prod_{v \in M_P} |\tfrac{1}{F(n')P^{n'}}|_v = n'^{\deg(F)} \prod_{v \in M_\infty} |P^{n'}|_v.$$

Now, we may apply the inequalities we found before for the archimedean values, obtaining:

$$\prod_{v \in M_\infty} |\alpha_v - \beta_n|_v \leq (\prod_{v \in M_\infty} |P|_v)^{-n'(1+\delta)}$$

and therefore

$$\prod_{v \in M_\infty \cup M_P} |\alpha_v - \beta_n|_v \leq (\prod_{v \in M_P} |\alpha_v - \beta_n|_v)^2 (\prod_{v \in M_\infty} |P|_v)^{-n'\delta)} \ll \mathrm{H}(\beta_n)^{-2-\frac{\delta}{2}}$$

Which is not possible due to the *Generalized Roth's Theorem.*

2. f has one pole.

Recall that we may modify f so that the inverse images of integral points are integral, and f is a polynomial of degree $d \geq 2$.
Suppose we have a sequence $\{t_n \in \mathcal{O}_k\}_{n\in\mathbb{N}}$ such that $f(t_n) = F(n')P^{n'}$. First we'll show f must be irreducible: if f had two distinct irreducible factors, say g and h, then $g(t_n)$ and $h(t_n)$ would grow exponentially and would be both divisible by increasing powers of P, tending to ∞ with n. As polynomials are continuous in the P-adic topology and ${\mathbb{P}^1}_{k_P}(k)$ is compact g and h would have a common zero in ${\mathbb{P}^1}_{k_P}$, and would not be coprime. So f is a power of an irreducible polynomial, say $f = h^m$. Then the solutions of $f(\alpha) = F(n)P^n$ are a subset of the solutions of one of the equations $F(n)P^b = cY^m$, for a fixed $c \in \mathcal{O}_k$ and $0 \leq b \leq m$. By extending k to a field k' such that $c^{\frac{1}{m}} \in \mathcal{O}_{k'}$, we may remove c, and apply Theorem (3.2.4). As all of the roots of F are simple, for $m > 1$ the solutions must be finite in number.
Factorize now $f = c\prod_{i=1,...,d}(x - \gamma_i)$, where γ_i are the (distinct) roots of f. Name L the decomposition field of f, which is an extension of k of degree at most $d!$. We want to understand the structure of the fractional ideals of $\mathcal{O}_L$ generated by $(t_n - \gamma_i)$. Recall $\mathcal{O}_L$ is a Dedekind domain, and let $I_1, ..., I_r$ be the factorization of the ideal generated by P. By comparing the ideal factorizations of $f(t_n)$ and $F(n')P^{n'}$, we may conclude that $\langle t_n - \gamma_i\rangle = A_{n,i}B_{n,i}$ where $A_{i,n}$ is a fractional ideal (with fixed denominator) whose norm is $\ll n'^{degF}$ and $B_{n,i}$ divides $\langle P\rangle^{n'}$. Then $B_{i,n}$ can be written ${I_1}^{n_{i,1}} \dots {I_r}^{n_{i,r}}$; We want to show this:

There is a partition $\Omega_1, ..., \Omega_s$ of $\{1, \dots, r\}$ such that, for infinitely many n:

- if $s \in \Omega_i, q \in \Omega_j$, then $I_s \neq I_q$.
- $n_{i,p}$ is bounded if $p \notin \Omega_i$.
- $|\Omega_i| = |\Omega_j|$ for all i, j.
- $n_{i,p} = n_{j,t}$ if $p \in \Omega_i, t \in \Omega_j$.

Set $\Omega_{i,n} = \{p \in 1, \dots, r | n_{i,p} \geq n\}$. First we show the $\Omega_{i,n}$ are eventually a partition; notice at once that, as the product of $B_{n,i}$ over i is an increasing ($\geq n$) power of the ideal $\langle P\rangle$, we must have $\cup_i \Omega_{i,n} = \{1, \dots, r\}$. Suppose $\Omega_{i,n} \cap \Omega_{j,n} \supseteq p$ for an infinite subset of $\mathbb{N}$, then $\gamma_i - \gamma_j = (t_n - \gamma_j) - (t_n - \gamma_i)$ belongs to ${I_p}^n$ for infinitely many n, which is impossible. Aslo, the ideals $I_1, \dots, I_r$ need not be distinct but $\{I_s \mid s \in \Omega_i\}$ and $\{I_s \mid s \in \Omega_j\}$ are disjoint if $i \neq j$.
As the set of partitions of $\{1, \dots, r\}$ is finite, we may choose a subsequence of $\mathbb{N}$ such that the partition $\Omega_{1,n}, ..., \Omega_{d,n}$ is always the same. By the same reasoning as before, if $p \notin \Omega_i$ then $n_{i,p}$ must be bounded, or else there would be γ_j such that $\gamma_i - \gamma_j$ belongs to arbitrary powers

of I_p. We now set $\Omega_i = \{p \in 1, \dots, r | n_{i,p} \quad \textit{is not bounded} \quad \}$, thus automatically fulfilling the last property.
The reason why $|\Omega_i| = |\Omega_j|$ is there is $\sigma \in \mathrm{Gal}(L/k)$ sending γ_i to γ_j, and correspondingly $\langle t_n - \gamma_i \rangle$ to $\langle t_n - \gamma_j \rangle$. As the Galois group acts on the set of prime factors of $\langle P \rangle$, the number of prime factors and their powers must remain unchanged.
Now, suppose $r, s \in \Omega_i$, $n_{i,q} \neq n_{i,s}$. Recall the action of the Galois group of L/k is transitive on the ideals $I_1, \dots, I_q$; so, choose any $\sigma \in \mathrm{Gal}(L/k)$ such that $\sigma(I_q) = I_s$. Then $\sigma(B_i) \neq B_i$, and thus $\sigma(\gamma_i) \neq \gamma_i$. But that would mean the Ω_i are not a partition, which we excluded before. Now, by permuting the γ_i we immediately obtain the second property.
With this result, we can let $A_{n,i}$ absorb the bounded components of $B_{n,i}$ whithout changing the growth of its norm, and write:

$$\langle t_n - \gamma_i \rangle = A_{n,i} (\textstyle\prod_{s \in \Omega_i} I_s)^{\tilde{n}}$$

Where $\tilde{n} = n_{i,r}$ for some i and some $r \in \Omega_i$, as they're all the same number.
Let us consider now the order of $\prod_{s \in \Omega_i} I_s$ in the *Ideal class group* of k; as the group is finite, the order is finite and as the Galois group acts transitively on those ideals it's the same for all i, say q. We may then write $A_{n,i} (\prod_{s \in \Omega_i} I_s)^{\tilde{n}} = A_{n,i} (\prod_{s \in \Omega_i} I_s)^{s_n} (\prod_{s \in \Omega_i} I_s)^{mq}$, where $s_n < q$. Then $(\prod_{s \in \Omega_i} I_s)^q = \langle \beta_i \rangle$, and as the ideal $\langle t_n - \gamma_i \rangle$ is principal, the fractional ideal $A_{n,i} (\prod_{s \in \Omega_i} I_s)^{s_n}$ must be principal too, or else the sum of their classes wouldn't be zero. We may then write $\langle t_{\tilde{n}} - \gamma_i \rangle = \alpha_{n,i} {\beta_i}^m$; now, $\beta_{1,n} \dots \beta_{d,n} = P^m c_n$, with c_n a unit of $\mathcal{O}_k$. Therefore, $\alpha_{1,n} \dots \alpha_{d,n} = F(n) {c_n}^{-1}$. Recall the $\alpha_{i,n}$ have fixed denominator: then factoring both the left hand and right hand term we conclude we may write $\alpha_{i,n} = \phi_{i,n} c_{i,n}$, where $\phi_{i,n}$ has its height bounded by $n^{\deg(F)}$ and $c_{i,n}$ is a unit.

We're now ready to conclude: choose γ_i, γ_j; possibly switching them and going to a subsequence, we may suppose $\prod_{s \in \Omega_i} |t_n - \gamma_i|_{v_{I_s}} \leq \prod_{p \in \Omega_j} |t_n - \gamma_j|_{v_{I_p}}$; consider now the fraction $\frac{t_n - \gamma_i}{t_n - \gamma_j}$:

$$\text{for all archimedean norms, we have:}$$
$$|1 - \tfrac{t_n - \gamma_i}{t_n - \gamma_j}|_v = |\tfrac{\gamma_i - \gamma_j}{t_n - \gamma_j}| \ll |P|_v^{-n\epsilon} \text{ for some } \epsilon > 0$$
$$\textstyle\prod_{s \in \Omega_i} |\frac{t_n - \gamma_i}{t_n - \gamma_j}|_{v_{I_s}} = (\prod_{v \in M_\infty} |\beta_i|_v)^{-m}$$
$$\textstyle\prod_{s \in \Omega_j} |\infty - \frac{t_n - \gamma_i}{t_n - \gamma_j}|_{v_{I_s}} = \prod_{s \in \Omega_j} |\frac{t_n - \gamma_j}{t_n - \gamma_i}|_{v_{I_s}} = (\prod_{v \in M_\infty} |\beta_j|_v)^{-m}.$$

Again, as for all archimedean absolute values the sequence β_n has 1 as a limit, the archimedean component of β_n's height is eventually bounded by any constant greater than one so that:

$$\mathrm{H}(\tfrac{t_n-\gamma_i}{t_n-\gamma_j}) \leq 2 \prod_{v \notin M_\infty} \max(1, |\tfrac{\alpha_{i,n}{\beta_i}^m}{\alpha_{j,n}{\beta_j}^m}|_v) \leq$$
$$2\,\mathrm{H}(\tfrac{\phi_{i,n}}{\phi_{j,n}}) \prod_{v \notin M_\infty} \max(1, |\tfrac{{\beta_i}^m}{{\beta_j}^m}|_v) \ll n^{2\deg(F)} (\prod_{v \in M_\infty} |\beta_j|_v)^m.$$

We can finally conclude:

$$\prod_{v \in M_\infty} |1 - \tfrac{t_n-\gamma_i}{t_n-\gamma_j}|_v \prod_{s \in \Omega_i} |\tfrac{t_n-\gamma_i}{t_n-\gamma_j}|_{v_{I_s}} \prod_{p \in \Omega_j} |\infty - \tfrac{t_n-\gamma_i}{t_n-\gamma_j}|_{v_{I_p}} \leq$$
$$\mathrm{H}(\tfrac{t_n-\gamma_i}{t_n-\gamma_j})^{-2-\frac{\epsilon}{2}}$$

For infinitely many n, which is not possible due to the *Generalized Roth's Theorem.*

□

Bibliography

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley series in mathematics, Westview Press (1994)

[2] J.W.S. Cassels, A. Fröhlich, Algebraic Number Theory, Academic Press (1967)

[3] Quing Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford graduate texts in Mathematics, Oxford university press (2002)

[4] Jean-Pierre Serre, *Lectures on the Mordell-Weil Theorem*, Aspects of Mathematics, F. Vieweg (1997)

[5] Serge Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag (1983)

[6] Serge Lang, *Diophantine Geometry*, Columbia University, New York (1962)

[7] Jean-Pierre Serre, *local fields*, Graduate Texts in Mathematics, Springer (1979)

[8] Umberto Zannier, *Some applications of Diophantine Approximation to Diophantine Equations*, Forum - Editrice Universitaria Udinese, Udine (2003)

[9] W.M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Springer-Verlag LNM 1467 (1991)

[10] Umberto Zannier, *Il Teorema di Irriducibilità di Hilbert*, lecture notes.

[11] Yuri Bilu, *A note on Universal Hilbert sets*, Journal für die reine und angewandte Mathematik, 479 (1996)

[12] Pierre Débes, Umberto Zannier, *Universal Hilbert subsets*, Mathematical Proceedings of the Cambridge Philosophical Society, 124, no.1 (1998)

[13] W.J. Le Veque, *On the equation* $y^m = f(x)$, Acta Arithmetica, 9 (1964)

[14] Támas Szamuely, *Galois groups and Fundamental groups*, Cambridge Studies in Advanced Mathematics, Cambridge University press (2008)

Aknowledgements

I wish to thank:

Professor Roberto Dvornicich, for the trust he put in me.

Professor Angelo Vistoli, for giving me the needed instruments for this work.

Professor Rocco Chirivì, for teaching me how to write of Mathematics.

Maurizio Monge, for the constant help he gave me during this year.